Diagonal mais curta

Seja P um polígono regular de k lados ($k > 6$), d a medida da sua diagonal mais curta e l a medida do seu lado. Supondo que d e l são comensuráveis, temos $d = mx$ e $l = nx$, onde m e n são inteiros positivos e x é uma medida comum a ambos. Poderemos, neste caso, encontrar uma sucessão estritamente decrescente de números inteiros positivos, de modo a chegar a um absurdo?

Vamos supor que, à semelhança das demonstrações anteriores, construíamos um novo polígono regular de k lados, P_1. Designando por d_1 a medida da sua diagonal e l_1 a medida do seu lado, suponhamos ainda que $l_1 = d - l$ e que $d_1 = a.d + b.l$ para alguns inteiros a e b. Por exemplo, se $a = -1$ e $b = 2$, então $d_1 = 2l - d$ e estamos no caso do quadrado. Para o pentágono regular temos $a = 0$ e $b = 1$ e, relativamente ao hexágono regular, temos $a = -1$ e $b = 3$.

Como $d = mx$ e $l = nx$, teríamos:

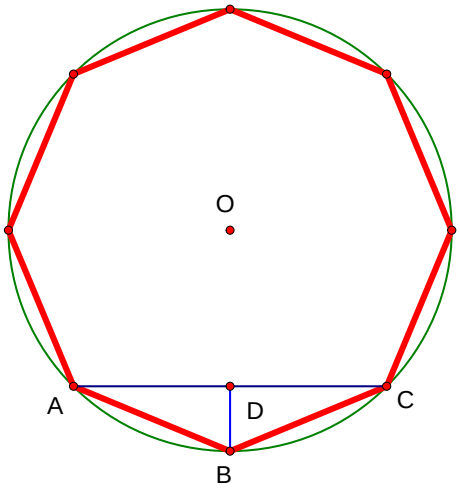
$$l_1 = d - l = mx - nx = (m - n)x = n_1 x$$

$$d_1 = a.d + b.l = amx + bnx = (am + bn)x = m_1 x$$

sendo $n_1 = m - n$ e $m_1 = am + bn$ dois números inteiros positivos, com $n_1 < n$. De facto, temos:

$$n_1 \geqslant n \Longrightarrow m - n \geqslant n \Longrightarrow m \geqslant 2n \Longrightarrow mx \geqslant 2nx \Longrightarrow d \geqslant 2l$$

o que é absurdo, uma vez que, em qualquer triângulo, cada lado tem um comprimento menor do que a soma do comprimento dos outros dois lados. Por exemplo, se considerarmos o triângulo $[ABC]$, vem $d = \overline{AC} < \overline{AB} + \overline{BC} = 2l$. Na verdade, marcando o ponto D, ponto médio do segmento $[AC]$, temos $\overline{AB} = \overline{BC} = l$, $\overline{AD} = \overline{DC} = \frac{d}{2}$ e $C\widehat{A}B = A\widehat{C}B = \frac{1}{2}.\frac{360^o}{k} = \frac{180^o}{k}$.



Logo, os triângulos $[ADB]$ e $[CDB]$ são congruentes, com $A\widehat{D}B = C\widehat{D}B = \frac{180^o}{2} = 90^o$, ou seja, são ambos rectângulos em D. Calculando o co-seno do ângulo $\measuredangle CAB$, temos:

$$\cos C\widehat{A}B = \cos\frac{180^o}{k} = \frac{\overline{AD}}{\overline{AB}} = \frac{\frac{d}{2}}{l} = \frac{d}{2l} \Longrightarrow d = 2l\cos\frac{180^o}{k} < 2l$$

Procedendo da mesma forma com o polígono P_1, obteríamos um novo polígono regular P_2 cuja diagonal seria $d_2 = m_2 x$ e cujo lado seria $l_2 = n_2 x$, sendo $n_2 = m_1 - n_1$ e $m_2 = am_1 + bn_1$ dois números inteiros positivos com $n_2 < n_1 < n$.

Continuando indefinidamente a contruir novos polígonos regulares, obteríamos uma sucessão estritamente decrescente de números inteiros positivos:

$$n_1 > n_2 > n_3 > n_4 > ...$$

tal que $n_i < n, \forall i \in \mathbb{N}$, o que é absurdo, dado que não pode haver uma infinidade de números inteiros positivos distintos menores do que n (de facto, existem exactamente $n-1$ elementos: 1,2,3,...,$n-2$, e $n-1$). Teríamos assim uma demonstração geométrica da incomensurabilidade entre a diagonal mais curta e o lado de um polígono regular qualquer com mais de 6 lados.

No entanto, como podemos garantir a existência dos inteiros a e b tais que $d_1 = a.d + b.l$?[1]

[1] Nota: mesmo supondo, mais geralmente, que $d_1 = a.d + b.l$ e $l_1 = c.d + e.l$ para alguns inteiros a, b, c, e e, viria da mesma forma que λ teria de ser solução de uma equação de grau 2 de coeficientes inteiros. Neste caso, teríamos:

De facto, as demonstrações geométricas anteriores não sugerem nenhum método geral para encontrar estes inteiros. Vejamos o que acontece, admitindo que tal é possível. Em cima, vimos que $d = 2l\cos\frac{180^o}{k}$, ou seja, $\frac{d}{l} = 2\cos\frac{180^o}{k}$. Analogamente, se considerarmos o polígono P_1, temos $\frac{d_1}{l_1} = 2\cos\frac{180^o}{k}$. Logo, tomando $\lambda = 2\cos\frac{180^o}{k}$, vem:

$$\lambda = \frac{d_1}{l_1} = \frac{a.d + b.l}{d - l} = \frac{a\frac{d}{l} + b}{\frac{d}{l} - 1} = \frac{a\lambda + b}{\lambda - 1} \Longrightarrow$$

$$\Longrightarrow \lambda(\lambda - 1) = a\lambda + b \Longrightarrow \lambda^2 - (a+1)\lambda - b = 0$$

Logo, λ teria de ser solução de uma equação de grau 2 de coeficientes inteiros.

Quando $k = 4$, vem $\lambda = 2\cos\frac{180^o}{4} = 2\cos 45^o = 2.\frac{\sqrt{2}}{2} = \sqrt{2}$, que é solução da equação $x^2 - 2 = 0 \qquad (a = -1,\ b = 2)$

Quando $k = 5$, vem $\lambda = 2\cos\frac{180^o}{5} = 2\cos 36^o = 2.\frac{\sqrt{5}+1}{4} = \frac{\sqrt{5}+1}{2}$, que é solução da equação $x^2 - x - 1 = 0 \qquad (a = 0,\ b = 1)$

Quando $k = 6$, vem $\lambda = 2\cos\frac{180^o}{6} = 2\cos 30^o = 2.\frac{\sqrt{3}}{2} = \sqrt{3}$, que é solução da equação $x^2 - 3 = 0 \qquad (a = -1,\ b = 3)$

Quando $k > 6$, demonstra-se que λ não pode ser solução de nenhuma equação de grau 2 de coeficientes inteiros. Logo, não existem a e b nas condições dadas e deixa de haver uma demonstração geométrica análoga às anteriores que prove a incomensurabilidade entre a diagonal mais curta e o lado de um polígono regular com mais de 6 lados.

De seguida, veremos porque é que λ não pode ser solução de nenhuma equação de grau 2 de coeficientes inteiros.

$$\lambda = \frac{d_1}{l_1} = \frac{a.d + b.l}{c.d + e.l} = \frac{a.\frac{d}{l} + b}{c.\frac{d}{l} + e} = \frac{a\lambda + b}{c\lambda + e} \Longrightarrow$$

$$\Longrightarrow \lambda(c\lambda + e) = a\lambda + b \Longrightarrow c\lambda^2 + (e - a)\lambda - b = 0$$

Vamos supor que $\lambda = 2\cos\frac{\pi}{k}$ é raiz da equação $ax^2 + bx + c = 0$, com a, b e c inteiros e $a \neq 0$.

Escrevendo $\lambda = 2\cos\frac{\pi}{k} = e^{\frac{\pi i}{k}} + e^{-\frac{\pi i}{k}} = t + t^{-1}$, com $t = e^{\frac{\pi i}{k}}$, vem:

$$
\begin{aligned}
& a\lambda^2 + b\lambda + c = 0 \iff \\
\iff & a\left(t + t^{-1}\right)^2 + b\left(t + t^{-1}\right) + c = 0 \iff \\
\iff & a\left(t^2 + 2 + t^{-2}\right) + b\left(t + t^{-1}\right) + c = 0 \iff \\
\iff & at^2 + bt + (2a + c) + bt^{-1} + at^{-2} = 0 \iff \\
\iff & \left(at^4 + bt^3 + (2a + c)t^2 + bt + a\right)t^{-2} = 0 \iff \\
\iff & at^4 + bt^3 + (2a + c)t^2 + bt + a = 0
\end{aligned}
$$

Portanto, t é raiz do polinómio $ax^4 + bx^3 + (2a + c)x^2 + bx + a$, de grau 4. Mas, por outro lado, demonstra-se que qualquer polinómio que tenha $e^{\frac{2\pi i}{n}}$ como raiz, com n um número inteiro positivo qualquer, tem grau não inferior a $\phi(n)$, onde $\phi(n)$ designa o número de elementos do conjunto $\{1, 2, 3, ..., n-1\}$ que são primos com n. Logo, como $t = e^{\frac{\pi i}{k}} = e^{\frac{2\pi i}{N}}$, onde $N = 2k$, temos necessariamente que $4 \geqslant \phi(N) = \phi(2k)$.

Decompondo N como produto de factores primos, temos $N = p_1^{i_1} p_2^{i_2} p_3^{i_3} ... p_l^{i_l}$, onde cada p_j é um número primo distinto e cada i_j é um número inteiro positvo. Então, $\phi(N)$ pode ser calculado pela seguinte fórmula:

$$\phi(N) = (p_1 - 1)(p_2 - 1)(p_3 - 1)...(p_l - 1)p_1^{i_1 - 1} p_2^{i_2 - 1} p_3^{i_3 - 1} ... p_l^{i_l - 1}$$

Para cada p_j divisor primo de N, temos que $p_j - 1$ divide $\phi(N)$, logo vem:

$p_j - 1 \leqslant 4 \Longrightarrow p_j \leqslant 5 \Longrightarrow p_j \in \{2, 3, 5\}$.

Supondo $N = 2^\alpha 3^\beta 5^\gamma$, vem:

Se $\gamma \geqslant 2$, $\phi(N) = \phi(2^\alpha 3^\beta 5^\gamma) = \phi(2^\alpha 3^\beta)\phi(5^\gamma) = \phi(2^\alpha 3^\beta).4.5^{\gamma-1} \geqslant 20$

Se $\gamma = 1$, $\phi(N) = \phi(2^\alpha 3^\beta .5) = \phi(2^\alpha 3^\beta)\phi(5) = \phi(2^\alpha 3^\beta).4$, logo vem:
$\phi(N) \leqslant 4 \Rightarrow \phi(2^\alpha 3^\beta) \leqslant 1 \Rightarrow 2^\alpha 3^\beta \in \{1, 2\} \Rightarrow N = 2^\alpha 3^\beta .5 \in \{5, 10\}$

Se $\gamma = 0$, então $N = 2^\alpha 3^\beta$ e vem:

Se $\beta \geqslant 2$, $\phi(N) = \phi(2^\alpha 3^\beta) = \phi(2^\alpha)\phi(3^\beta) = \phi(2^\alpha).2.3^{\beta-1} \geqslant 6$
Se $\beta = 1$, $\phi(N) = \phi(2^\alpha .3) = \phi(2^\alpha).2$, logo vem:
$\phi(N) \leqslant 4 \Rightarrow \phi(2^\alpha) \leqslant 2 \Rightarrow 2^\alpha \in \{1, 2, 4\} \Rightarrow N = 2^\alpha .3 \in \{3, 6, 12\}$
Se $\beta = 0$, então $N = 2^\alpha$ e vem:
$\phi(N) \leqslant 4 \Rightarrow \phi(2^\alpha) \leqslant 4 \Rightarrow N = 2^\alpha \in \{1, 2, 4, 8\}$

Logo, $N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Como $N = 2k$, temos que $k \in \{1, 2, 3, 4, 5, 6\}$, sendo estes os únicos valores possíveis de modo a que λ seja raiz de um polinómio de grau 2 de coeficientes inteiros. Para $k > 6$, λ não pode ser raiz de nenhuma equação do segundo grau de coeficientes inteiros.

Como poderemos demonstrar a incomensurabilidade entre o lado e a diagonal mais curta de um polígono regular com mais de 6 lados?

Apesar de não podermos utilizar o mesmo tipo de argumentação geométrica que foi usado no caso do quadrado, do pentágono regular e do hexágono regular para justificar a incomensurabilidade entre o lado e a diagonal mais curta de um polígono regular com mais de 6 lado, tal não significa que ela não se verifique mesmo nestes casos. Assim, da mesma maneira que utilizamos conhecimentos algébricos para demonstrar esta impossibilidade de generalização das demonstrações anteriores, podemos agora recorrer a estes conhecimentos para obter uma demonstração não geométrica da incomensurabilidade entre o lado e a diagonal mais curta de um qualquer polígono regular com 4 ou mais lados.

De facto, tal problema é equivalente a demonstrar que a razão entre a diagonal mais curta e o lado de um polígono regular de n lados, com $n \geqslant 4$, é um número irracional. Atrás, vimos que esta razão era $\lambda = 2\cos\frac{\pi}{k} = e^{\frac{\pi i}{k}} + e^{-\frac{\pi i}{k}} = t + t^{-1}$, com $t = e^{\frac{\pi i}{k}}$, sendo que t era raiz de um único polinómio $f(x)$ mónico de coeficientes inteiros, irredutível e que dividia todos os polinómios de coeficientes racionais do quais t era raiz. Supondo, por redução ao absurdo, que λ era racional, viria:

$$t+t^{-1} = \lambda \iff (t+t^{-1})t = \lambda t \iff t^2+1 = \lambda t \iff t^2-\lambda t+1 = 0 \iff f(t) = 0$$

onde $f(x) = x^2 + (1-\lambda)x + 1$ é um polinómio mónico de coeficientes racionais do qual t é raiz e de grau 2. Mas, já vimos que o menor grau possível para um polinómio nessas condições era $\phi(2k)$, pelo que viria $\phi(2k) \leqslant 2$. Escrevendo $N = 2k = p_1^{i_1}p_2^{i_2}p_3^{i_3}...p_l^{i_l}$, temos:

$$\phi(N) = (p_1-1)(p_2-1)(p_3-1)...(p_l-1)p_1^{i_1-1}p_2^{i_2-1}p_3^{i_3-1}...p_l^{i_l-1}$$

Logo, se p_j é um primo que divide N, então $p_j - 1$ divide $\phi(N)$. Como $\phi(N) \leqslant 2 \Rightarrow p_j - 1 \leqslant 2 \Rightarrow p_j \leqslant 3$, temos que os únicos divisores primos possíveis de N são 2 e 3. Supondo $N = 2^\alpha 3^\beta$, vem:

Se $\beta \geqslant 2$, $\phi(N) = \phi(2^\alpha 3^\beta) = \phi(2^\alpha)\phi(3^\beta) = \phi(2^\alpha).2.3^{\beta-1} \geqslant 6$
Se $\beta = 1$, $\phi(N) = \phi(2^\alpha.3) = \phi(2^\alpha).2$, logo vem:
$\phi(N) \leqslant 2 \Rightarrow \phi(2^\alpha) \leqslant 1 \Rightarrow 2^\alpha \in \{1,2\} \Rightarrow N = 2^\alpha.3 \in \{3,6\}$
Se $\beta = 0$, então $N = 2^\alpha$ e vem:
$\phi(N) \leqslant 2 \Rightarrow \phi(2^\alpha) \leqslant 2 \Rightarrow N = 2^\alpha \in \{1,2,4\}$

Logo, $N \in \{1,2,3,4,6\}$. Como $N = 2k$, temos que $k \in \{1,2,3\}$, o que é absurdo pois $k \geqslant 4$. Conclui-se assim que λ não pode ser um número racional.

De seguida, veremos porque é que o grau mínimo de um polinómio que tenha $e^{\frac{2\pi i}{n}}$ como raiz é $\phi(n)$.

Dado um número complexo qualquer, se ele for raiz de um polinómio de coeficientes racionais, então existe um polinómio mónico, de coeficientes racionais e irredutível, que divide todos os outros polinómios de coeficientes racionais dos quais esse número é raiz e que, além disso, é o único polinómio nestas condições. Em particular, se considerarmos o número complexo $t = e^{\frac{2\pi i}{n}}$, como $t^n = e^{2\pi i} = 1$, vem que t é raiz do polinómio $x^n - 1$. Pelo lema de Gauss, o polinómio $x^n - 1$ pode ser escrito como produto de polinómios irredutíveis de coeficientes inteiros. Além disso, como $x^n - 1$ é mónico, esses factores são necessariamente mónicos. Pela lei do anulamento do produto, pelo menos um desses factores anula-se em t. Designando esse polinómio por $f(x)$, temos que $f(x)$ é um polinómio mónico, de coeficientes inteiros, irredutível e que divide todos os outros polinómios de coeficientes racionais dos quais t é raiz.

Exemplos:
$x^2-1 = (x-1)(x+1)$ e $f(x) = x+1$ é tal que $f(e^{\frac{2\pi i}{2}}) = f(e^{\pi i}) = f(-1) = 0$

$x^3 - 1 = (x-1)(x^2+x+1)$ e $f(x) = x^2 + x + 1$ é tal que $f(e^{\frac{2\pi i}{3}}) = f\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 0$

$x^4 - 1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$ e $f(x) = x^2 + 1$ é tal que $f(e^{\frac{2\pi i}{4}}) = f(i) = 0$

$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$ e $f(x) = x^4 + x^3 + x^2 + x + 1$ é tal que $f(e^{\frac{2\pi i}{5}}) = f\left(\frac{\sqrt{5}-1}{4} + \sqrt{\frac{5+\sqrt{5}}{8}}i\right) = 0$

$x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ e $f(x) = x^2 - x + 1$ é tal que $f(e^{\frac{2\pi i}{6}}) = f(e^{\frac{\pi i}{3}}) = f\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 0$

Veremos agora que $f(x)$ tem, pelo menos, $\phi(n)$ raízes complexas distintas. Para cada $j \in \{1, 2, 3, ..., n-1\}$ tal que $(j, n) = 1$, se aplicarmos o algoritmo da divisão aos polinómios $f(x^j)$ e $f(x)$, ambos mónicos e de coeficientes inteiros, obtemos $f(x^j) = q_j(x)f(x) + r_j(x)$ para alguns polinómios $q_j(x)$ e $r_j(x)$ de coeficientes inteiros, com $r_j(x) = 0$ ou de grau inferior ao de $f(x)$. Seja M um número inteiro superior ao valor absoluto de todos os coeficientes dos polinómios $r_j(x)$. Para todo o primo p que não divide n e é maior do que M, vejamos que $f(x)$ divide $f(x^p)$. Sendo s o resto da divisão de p por n, temos que $s \in \{1, 2, 3, ..., n-1\}$ e $(s, n) = (p, n) = 1$. Logo, vem:

$f(x^s) = q_s(x)f(x) + r_s(x)$, com $r_s(x) = 0$ ou de grau inferior ao de $f(x)$.

$f(x)^p = f(x^p) + p.g(x)$ para algum polinómio $g(x)$ de coeficientes inteiros[2].

$g(x) = u(x)f(x) + v(x)$ para alguns polinómios $u(x)$ e $v(x)$ de coeficientes inteiros, com $v(x) = 0$ ou de grau inferior ao de $f(x)$.

Para $x = t$, vem:

$f(t^s) = q_s(t)f(t) + r_s(t) \Longrightarrow f(t^s) = r_s(t)$
$g(t) = u(t)f(t) + v(t) \Longrightarrow g(t) = v(t)$
$f(t)^p = f(t^p) + p.g(t) \Longrightarrow 0 = f(t^p) + p.v(t) \Longrightarrow f(t^p) = -p.v(t)$

Como $p = nq + s$ para algum inteiro q e $t^n = 1$, vem: $t^p = t^{nq+s} = (t^n)^q\, t^s = t^s \Longrightarrow f(t^p) = f(t^s) \Longrightarrow -p.v(t) = r_s(t) \Longrightarrow p.v(t) + r_s(t) = 0$, pelo que t é raiz do polinómio $p.v(x) + r_s(x)$ e, portanto, $f(x)$ divide $p.v(x) + r_s(x)$. Sendo $v(x)$ e $r_s(x)$ dois polinómios nulos ou de grau inferior ao grau de $f(x)$, o polinómio $p.v(x) + r_s(x)$ também é nulo ou de grau inferior ao grau de $f(x)$. Mas, como $f(x)$ divide o polinómio $p.v(x) + r_s(x)$, o seu grau não pode ser inferior ao grau de $f(x)$, logo $p.v(x) + r_s(x) = 0$, ou seja, $r_s(x) = -p.v(x)$, pelo que todos os coeficientes de $r_s(x)$ são múltiplos inteiros de p. Além disso, sendo $s \in \{1, 2, 3, ..., n-1\}$ e $(s, n) = 1$, todos os coeficientes do polinómio $r_s(x)$ são, em valor absoluto, inferiores a M, logo inferiores a p, de onde se conclui que são todos nulos, isto é, $r_s(x) = 0$. Temos então: $r_s(x) = 0 \Longrightarrow -p.v(x) = 0 \Longrightarrow v(x) = 0 \Longrightarrow g(x) = u(x)f(x) \Longrightarrow f(x)^p = f(x^p) + p.u(x)f(x) \Longrightarrow f(x^p) = f(x)^p - p.u(x)f(x) = [f(x)^{p-1} - p.u(x)]f(x)$, ou seja, $f(x)$ divide $f(x^p)$.

Seja $J = j + nP$ onde P é o produto de todos os primos menores ou iguais a M que não dividem j. Note-se que $(J, n) = (j, n) = 1$. Então,

[2] Seja $f(x) = \sum_{i=0}^{n} a_i x^i$ um polinómio de coeficientes inteiros e p um número primo.Temos:

$$\begin{aligned}
f(x)^p &= \left(\sum_{i=0}^{n} a_i x^i\right)^p = (a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0)^p = \\
&= \sum_{\substack{p_0+p_1+...+p_n=p \\ p_0,p_1,...,p_n \geqslant 0}} \frac{p!}{p_0!p_1!...p_n!} {a_0}^{p_0}(a_1 x)^{p_1}...(a_n x^n)^{p_n} = \\
&= \sum_{i=0}^{n}(a_i x^i)^p + \sum_{\substack{p_0+p_1+...+p_n=p \\ 0 \leqslant p_0,p_1,...,p_n \leqslant p-1}} \frac{p!}{p_0!p_1!...p_n!} {a_0}^{p_0}(a_1 x)^{p_1}...(a_n x^n)^{p_n} = \\
&= \sum_{i=0}^{n} a_i x^{ip} + \sum_{i=0}^{n}(a_i^p - a_i)x^{ip} + \sum_{\substack{p_0+p_1+...+p_n=p \\ 0 \leqslant p_0,p_1,...,p_n \leqslant p-1}} \frac{p(p-1)!}{p_0!p_1!...p_n!} {a_0}^{p_0}(a_1 x)^{p_1}...(a_n x^n)^{p_n} = \\
&= f(x^p) + p.g(x)
\end{aligned}$$

onde

$$g(x) = \sum_{i=0}^{n} \frac{a_i^p - a_i}{p} x^{ip} + \sum_{\substack{p_0+p_1+...+p_n=p \\ 0 \leqslant p_0,p_1,...,p_n \leqslant p-1}} \frac{(p-1)!}{p_0!p_1!...p_n!} {a_0}^{p_0}(a_1 x)^{p_1}...(a_n x^n)^{p_n}$$

é um polinómio de coeficientes inteiros (pelo pequeno teorema de Fermat, $x^p - x$ é sempre múltiplo de p para todo o x inteiro e p primo).

$t^J = t^{j+nP} = t^j \left(t^n\right)^P = t^j$ e, escrevendo J como um produto de primos $p_1 p_2 ... p_m$ (não necessariamente distintos), cada primo p_i não divide n e é maior do que M. De facto, se houvesse um divisor primo de J menor ou igual a M, teria de ser divisor de P ou de j, mas não de ambos, por definição de P. Mas, sendo divisor de J e de P, também seria divisor de $j = J - nP$; sendo divisor de J e de j, também seria divisor de $nP = J - j$, logo seria divisor de P uma vez que j e n são primos entre si. Logo, não há divisores primos de J menores ou iguais a M.

Então, pelo que vimos anteriormente, podemos concluir que $f(x)$ divide $f(x^{p_1})$ e, como t é raiz de $f(x)$, também é raiz de $f(x^{p_1})$, ou seja, $f(t^{p_1}) = 0$. Como $f(x)$ divide $f(x^{p_2})$ e t^{p_1} é raiz de $f(x)$, também é raiz de $f(x^{p_2})$, ou seja, $f\left((t^{p_1})^{p_2}\right) = f(t^{p_1 p_2}) = 0$. Novamente, como $f(x)$ divide $f(x^{p_3})$ e $t^{p_1 p_2}$ é raiz de $f(x)$, também é raiz de $f(x^{p_3})$, ou seja, $f\left((t^{p_1 p_2})^{p_3}\right) = f(t^{p_1 p_2 p_3}) = 0$. Continuando este processo, obtemos $f(t^{p_1 p_2 \cdots p_m}) = f(t^J) = f(t^j) = 0$, pelo que t^j é raiz de $f(x)$ para todo j tal que $(j, n) = 1$. Então, o polinómio $f(x)$ tem, pelo menos, $\phi(n)$ raízes complexas distintas, dado que todos os números complexos da forma t^j, com $j \in \{1, 2, 3, ..., n-1\}$, são distintos ($t^j = e^{\frac{2j\pi}{n} i}$ é o número complexo de módulo 1 e argumento $\frac{2j\pi}{n} \in]0, 2\pi[$). Portanto, o seu grau terá de ser maior ou igual a $\phi(n)$, assim como o grau de todos os polinómios de coeficientes racionais dos quais t é raiz.

Lema de Gauss:

Se um polinómio de coeficientes inteiros puder ser escrito como produto de dois polinómios de coeficientes racionais, então também pode ser escrito como produto de dois polinómios de coeficientes inteiros.

Generalizando, se um polinómio de coeficientes inteiros puder ser escrito como produto de n polinómios de coeficientes racionais, então também pode ser escrito como produto de n polinómios de coeficientes inteiros, o que pode ser visto por indução.

Suponhamos que o resultado é válido para um produto de $n-1$ polinómios de coeficientes racionais e seja $f = f_1 f_2 ... f_{n-1} f_n$ um produto de $n-1$ polinómios de coeficientes racionais. Tomando $g = f_1 f_2 ... f_{n-1}$, temos que $f = g.f_n$, sendo g e f_n polinómios de coeficientes racionais. Pelo lema de Gauss, existem dois polinómios de coeficientes inteiros $g\prime$ e f'_n tais que $f = g'.f'_n$. Além disso, deduz-se da demonstração deste lema que existe um racional r tal que $g\prime = rg$ e $f'_n = \frac{1}{r} f_n$, pelo que $g\prime$ é ainda um produto de $n-1$ polinómios de coeficientes racionais. Aplicando a hipótese de indução, temos $g' = f'_1 f'_2 ... f'_{n-1}$, onde f'_i é um polinómio de coeficientes inteiros para todo $i \in \{1, 2, ..., n-1\}$. Logo, vem $f = g'.f'_n = f'_1 f'_2 ... f'_{n-1} f'_n$ e f pode ser escrito como produto de n polinómios de coeficientes inteiros.