Demostracions Euclidianes de la infinitud de primers en progressions aritmètiques

Joan Arenillas i Cases

Universitat Autònoma de Barcelona
Grau en Matemàtiques

4 de juliol de 2025

Introducció I

Euclides va demostrar al voltant de l'any 300 aC que hi ha infinits primers.

Introducció I

Euclides va demostrar al voltant de l'any 300 aC que hi ha infinits primers.

Demostració.

Suposem que hi ha finits primers: $p_1, p_2, \ldots, p_m$. Considerem el número $Q := p_1 p_2 \cdots p_m + 1 > 1$, que té almenys un divisor primer.

Introducció I

Euclides va demostrar al voltant de l'any 300 aC que hi ha infinits primers.

Demostració.

Suposem que hi ha finits primers: $p_1, p_2, \ldots, p_m$. Considerem el número $Q := p_1 p_2 \cdots p_m + 1 > 1$, que té almenys un divisor primer. Però Q no és divisible per cap dels primers de la llista finita, contradicció. $\square$

Introducció II

Considerem la progressió aritmètica $kn + \ell$, per $n \geqslant 0$, on $k, \ell \in \mathbb{Z}^+$.

Introducció II

Considerem la progressió aritmètica $kn + \ell$, per $n \geqslant 0$, on $k, \ell \in \mathbb{Z}^+$.

Si k i ℓ són coprimers, el Teorema de Dirichlet ens diu que hi ha infinits primers $\equiv \ell \pmod{k}$.

Introducció II

Considerem la progressió aritmètica $kn + \ell$, per $n \geqslant 0$, on $k, \ell \in \mathbb{Z}^+$.

Si k i ℓ són coprimers, el Teorema de Dirichlet ens diu que hi ha infinits primers $\equiv \ell \pmod{k}$.

Ens preguntem:

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració que segueixi *l'esperit d'Euclides*?

Introducció II

Considerem la progressió aritmètica $kn + \ell$, per $n \geqslant 0$, on $k, \ell \in \mathbb{Z}^+$.

Si k i ℓ són coprimers, el Teorema de Dirichlet ens diu que hi ha infinits primers $\equiv \ell \pmod{k}$.

Ens preguntem:

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració que segueixi *l'esperit d'Euclides*?

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi aquestes demostracions?

Introducció II

Considerem la progressió aritmètica $kn + \ell$, per $n \geqslant 0$, on $k, \ell \in \mathbb{Z}^+$.

Si k i ℓ són coprimers, el Teorema de Dirichlet ens diu que hi ha infinits primers $\equiv \ell \pmod{k}$.

Ens preguntem:

- P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració que segueixi *l'esperit d'Euclides*?
- P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi aquestes demostracions?

L'objectiu del treball és respondre les preguntes P1 i P2.

Introducció III

Cal fer la pregunta P1 precisa.

Cal fer la pregunta P1 precisa.

Exemple

Existeixen infinits primers $\equiv 1 \pmod 3$.

Introducció III

Cal fer la pregunta P1 precisa.

Exemple

Existeixen infinits primers $\equiv 1 \pmod 3$.

Demostració.

Suposem que hi ha només finits primers $\equiv 1 \pmod 3$: $p_1, p_2, \ldots, p_m$. Considerem $Q := p_1 p_2 \cdots p_m$ i el polinomi $f(x) := x^2 + 3$. Ara, $f(Q) = Q^2 + 3$ té almenys un divisor primer, p, ja que és més gran que 1.

Introducció III

Cal fer la pregunta P1 precisa.

Exemple

Existeixen infinits primers $\equiv 1 \pmod 3$.

Demostració.

Suposem que hi ha només finits primers $\equiv 1 \pmod 3$: $p_1, p_2, \ldots, p_m$. Considerem $Q := p_1 p_2 \cdots p_m$ i el polinomi $f(x) := x^2 + 3$. Ara, $f(Q) = Q^2 + 3$ té almenys un divisor primer, p, ja que és més gran que 1.

Si $p = p_i$ per a algun i, llavors p divideix Q^2. Com que p també divideix $Q^2 + 3$, p divideix 3, per tant $p = p_i = 3$, contradicció. Per tant, p és un primer que no es troba a la nostra llista.

Introducció III

Cal fer la pregunta P1 precisa.

Exemple

Existeixen infinits primers $\equiv 1 \pmod 3$.

Demostració.

Suposem que hi ha només finits primers $\equiv 1 \pmod 3$: $p_1, p_2, \ldots, p_m$. Considerem $Q := p_1 p_2 \cdots p_m$ i el polinomi $f(x) := x^2 + 3$. Ara, $f(Q) = Q^2 + 3$ té almenys un divisor primer, p, ja que és més gran que 1.
Si $p = p_i$ per a algun i, llavors p divideix Q^2. Com que p també divideix $Q^2 + 3$, p divideix 3, per tant $p = p_i = 3$, contradicció. Per tant, p és un primer que no es troba a la nostra llista.
Si p divideix $Q^2 + 3$, llavors $Q^2 \equiv -3 \pmod p$. Això vol dir que $p \equiv 1 \pmod 3$, cosa que ens proporciona una infinitat de nombres primers $\equiv 1 \pmod 3$ sempre que en tinguem un. $\square$

Introducció IV

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Introducció IV

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Un primer p és *divisor primer* de $f \in \mathbb{Z}[x]$ si $p \mid f(m)$ per algun $m \in \mathbb{Z}$.

Introducció IV

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Un primer p és *divisor primer* de $f \in \mathbb{Z}[x]$ si $p \mid f(m)$ per algun $m \in \mathbb{Z}$.

Definició

Diem que la progressió aritmètica $\equiv \ell \pmod{k}$ admet un polinomi Euclidià *si existeix un polinomi irreductible* $f \in \mathbb{Z}[x]$ *tal que els seus divisors primers, excepte un nombre finit, són* $\equiv 1, \ell \pmod{k}$, *amb infinits primers de l'últim tipus.*

Introducció IV

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Un primer p és *divisor primer* de $f \in \mathbb{Z}[x]$ si $p \mid f(m)$ per algun $m \in \mathbb{Z}$.

Definició

Diem que la progressió aritmètica $\equiv \ell \pmod{k}$ admet un polinomi Euclidià *si existeix un polinomi irreductible* $f \in \mathbb{Z}[x]$ *tal que els seus divisors primers, excepte un nombre finit, són* $\equiv 1, \ell \pmod{k}$, *amb infinits primers de l'últim tipus.*

Si utilitzem aquest polinomi Euclidià per demostrar la infinitud de primers $\equiv \ell \pmod{k}$, tindrem una *demostració Euclidiana*.

Part teòrica

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Part teòrica

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració Euclidiana?

Una part de la pregunta ens la resol Schur [2].

Teorema (Schur, 1912)

Si $\ell^2 \equiv 1 \pmod{k}$, llavors existeix una demostració Euclidiana del fet que hi ha infinits primers $\equiv \ell \pmod{k}$.

Una mica de notació:

- Fixem $k \geqslant 3$.

Una mica de notació:

- Fixem $k \geqslant 3$.
- Fixem $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ que compleixi $\ell^2 \equiv 1 \pmod{k}$.

Teorema de Schur

Una mica de notació:

- Fixem $k \geqslant 3$.
- Fixem $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ que compleixi $\ell^2 \equiv 1 \pmod{k}$.
- Considerem $\{1, \ell\} \leqslant (\mathbb{Z}/k\mathbb{Z})^\times$.

Una mica de notació:

- Fixem $k \geqslant 3$.
- Fixem $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ que compleixi $\ell^2 \equiv 1 \pmod{k}$.
- Considerem $\{1, \ell\} \leqslant (\mathbb{Z}/k\mathbb{Z})^\times$.
- Definim S com el conjunt de representants de les classes laterals de $\{1, \ell\}$ en $(\mathbb{Z}/k\mathbb{Z})^\times$.

Una mica de notació:

- Fixem $k \geqslant 3$.
- Fixem $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ que compleixi $\ell^2 \equiv 1 \pmod{k}$.
- Considerem $\{1, \ell\} \leqslant (\mathbb{Z}/k\mathbb{Z})^\times$.
- Definim S com el conjunt de representants de les classes laterals de $\{1, \ell\}$ en $(\mathbb{Z}/k\mathbb{Z})^\times$.
- Fixem ζ, una arrel k-èssima primitiva de la unitat i $u \in \mathbb{Z}$.

Teorema de Schur

Una mica de notació:

- Fixem $k \geqslant 3$.
- Fixem $\ell \in (\mathbb{Z}/k\mathbb{Z})^\times$ que compleixi $\ell^2 \equiv 1 \pmod{k}$.
- Considerem $\{1, \ell\} \leqslant (\mathbb{Z}/k\mathbb{Z})^\times$.
- Definim S com el conjunt de representants de les classes laterals de $\{1, \ell\}$ en $(\mathbb{Z}/k\mathbb{Z})^\times$.
- Fixem ζ, una arrel k-èssima primitiva de la unitat i $u \in \mathbb{Z}$.

Considerem el polinomi

$$f_u(x) := \prod_{s \in S} \left(x - (\zeta^s - u)(u - \zeta^{\ell s})\right).$$

El polinomi $f_u \in \mathbb{Z}[x]$ serà el nostre polinomi Euclidià.

Proposició

Excepte finits valors d'u, el polinomi f_u genera el cos fix per $\{1, \ell\}$ i és irreductible.

Teorema de Schur

El polinomi $f_u \in \mathbb{Z}[x]$ serà el nostre polinomi Euclidià.

Proposició

Excepte finits valors d'u, el polinomi f_u genera el cos fix per $\{1, \ell\}$ i és irreductible.

Teorema (Schur)

Tots els divisors primers de f_u són $\equiv 1, \ell \pmod{k}$ (excepte un nombre finit de primers).

Teorema de Schur

El polinomi $f_u \in \mathbb{Z}[x]$ serà el nostre polinomi Euclidià.

Proposició

Excepte finits valors d'u, el polinomi f_u genera el cos fix per $\{1, \ell\}$ i és irreductible.

Teorema (Schur)

Tots els divisors primers de f_u són $\equiv 1, \ell \pmod{k}$ (excepte un nombre finit de primers).

Proposició

Qualsevol primer que sigui $\equiv 1, \ell \pmod{k}$ divideix f_u.

Teorema de Schur

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Teorema

Si existeix un primer $p \equiv \ell \pmod{k}$*, llavors existeix una demostració Euclidiana de la infinitud de primers* $\equiv \ell \pmod{k}$*.*

Teorema de Schur

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Teorema

Si existeix un primer $p \equiv \ell \pmod{k}$, *llavors existeix una demostració Euclidiana de la infinitud de primers* $\equiv \ell \pmod{k}$.

Aquest teorema ens dona un *argument general* que podem implementar.

Teorema de Schur

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Teorema

Si existeix un primer $p \equiv \ell \pmod{k}$, llavors existeix una demostració Euclidiana de la infinitud de primers $\equiv \ell \pmod{k}$.

Aquest teorema ens dona un *argument general* que podem implementar. Hem trobat una demostració *sistemàtica* i *Euclidiana*, però no elemental (de moment).

Teorema de Schur

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Teorema

Si existeix un primer $p \equiv \ell \pmod{k}$*, llavors existeix una demostració Euclidiana de la infinitud de primers* $\equiv \ell \pmod{k}$*.*

Aquest teorema ens dona un *argument general* que podem implementar. Hem trobat una demostració *sistemàtica* i *Euclidiana*, però no elemental (de moment).

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració que segueixi l'esperit d'Euclides?

Teorema de Schur

Això ens diu que f_u és un polinomi Euclidià per la nostra demostració Euclidiana.

Teorema

Si existeix un primer $p \equiv \ell \pmod{k}$*, llavors existeix una demostració Euclidiana de la infinitud de primers* $\equiv \ell \pmod{k}$*.*

Aquest teorema ens dona un *argument general* que podem implementar. Hem trobat una demostració *sistemàtica* i *Euclidiana*, però no elemental (de moment).

Recordem

P1 Quan hi hagi infinits primers $\equiv \ell \pmod{k}$, quan es pot trobar una demostració que segueixi l'esperit d'Euclides?

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi aquestes demostracions?

El recíproc ens el dona Murty [1].

Teorema (Murty, 1988)

Si existeix un polinomi Euclidià per la progressió aritmètica $\equiv \ell \pmod{k}$, *llavors* $\ell^2 \equiv 1 \pmod{k}$.

Teorema de Murty

El recíproc ens el dona Murty [1].

Teorema (Murty, 1988)

Si existeix un polinomi Euclidià per la progressió aritmètica $\equiv \ell \pmod{k}$*, llavors* $\ell^2 \equiv 1 \pmod{k}$.

Fixem un cos de nombres K. Necessitem definir els conjunts

$$\mathrm{Spl}_1(K) := \{p \text{ primer} : p \text{ té un factor ideal primer en } K \\ \text{amb } \mathbb{Z}/p\mathbb{Z} \text{ com a cos residual}\},$$

El recíproc ens el dona Murty [1].

Teorema (Murty, 1988)

Si existeix un polinomi Euclidià per la progressió aritmètica $\equiv \ell \pmod{k}$, *llavors* $\ell^2 \equiv 1 \pmod{k}$.

Fixem un cos de nombres K. Necessitem definir els conjunts

$$\mathrm{Spl}_1(K) := \{p \text{ primer} : p \text{ té un factor ideal primer en } K \\ \text{amb } \mathbb{Z}/p\mathbb{Z} \text{ com a cos residual}\},$$

$$S_1(k, K) := \{b \bmod k : p \equiv b \pmod{k} \text{ per infinits } p \in \mathrm{Spl}_1(K)\}.$$

Teorema de Murty

El recíproc ens el dona Murty [1].

Teorema (Murty, 1988)

Si existeix un polinomi Euclidià per la progressió aritmètica $\equiv \ell \pmod{k}$*, llavors* $\ell^2 \equiv 1 \pmod{k}$.

Fixem un cos de nombres K. Necessitem definir els conjunts

$$\begin{gathered}\mathrm{Spl}_1(K) := \{p \text{ primer} : p \text{ té un factor ideal primer en } K \\ \text{amb } \mathbb{Z}/p\mathbb{Z} \text{ com a cos residual}\},\end{gathered}$$

$$S_1(k, K) := \{b \bmod k : p \equiv b \pmod{k} \text{ per infinits } p \in \mathrm{Spl}_1(K)\}.$$

Cal veure que $S_1(k, K)$ és un *subgrup* de $(\mathbb{Z}/k\mathbb{Z})^\times$ passant pel Teorema de Densitat de Chebotarev.

Els teoremes de Schur i Murty ens permeten resoldre completament la pregunta P1.✓

Teorema de Murty

Els teoremes de Schur i Murty ens permeten resoldre completament la pregunta P1.✓

Teorema (Murty i Schur)

Existeix una demostració Euclidiana del fet que hi ha infinits primers $\equiv \ell \pmod{k}$ *si i només si* $\ell^2 \equiv 1 \pmod{k}$.

Teorema de Murty

Els teoremes de Schur i Murty ens permeten resoldre completament la pregunta P1.✓

Teorema (Murty i Schur)

Existeix una demostració Euclidiana del fet que hi ha infinits primers $\equiv \ell \pmod{k}$ *si i només si* $\ell^2 \equiv 1 \pmod{k}$.

A més, hem trobat un mètode *sistemàtic*. Quan l'implementem veurem que és *elemental*.

Conseqüència: caracterització de $\mathrm{Spl}_1(L)$

Recordem que el polinomi f_u genera el cos fix per $\{1, \ell\}$, diem-li L.

Conseqüència: caracterització de $\mathrm{Spl}_1(L)$

Recordem que el polinomi f_u genera el cos fix per $\{1, \ell\}$, diem-li L.

Els divisors primers del polinomi f_u són (excepte finits casos):

$$\{p \text{ primer} : p \equiv 1, \ell \pmod{k}\}.$$

Conseqüència: caracterització de $\mathrm{Spl}_1(L)$

Recordem que el polinomi f_u genera el cos fix per $\{1, \ell\}$, diem-li L.

Els divisors primers del polinomi f_u són (excepte finits casos):

$$\{p \text{ primer} : p \equiv 1, \ell \pmod{k}\}.$$

Hem caracteritzat, a través del Criteri de Dedekind, el conjunt $\mathrm{Spl}_1(L)$:

Llei de reciprocitat

$$\mathrm{Spl}_1(L) \simeq \{p \text{ primer} : p \equiv 1, \ell \pmod{k}\}.$$

Conseqüència: caracterització de $\mathrm{Spl}_1(L)$

Recordem que el polinomi f_u genera el cos fix per $\{1, \ell\}$, diem-li L.

Els divisors primers del polinomi f_u són (excepte finits casos):

$$\{p \text{ primer} : p \equiv 1, \ell \pmod{k}\}.$$

Hem caracteritzat, a través del Criteri de Dedekind, el conjunt $\mathrm{Spl}_1(L)$:

Llei de reciprocitat

$$\mathrm{Spl}_1(L) \simeq \{p \text{ primer} : p \equiv 1, \ell \pmod{k}\}.$$

Caracteritzacions de $\mathrm{Spl}_1(L)$ es coneixen si L és un cos ciclotòmic o si $[L : \mathbb{Q}] = 2$. En el nostre cas, $[\mathbb{Q}(\zeta) : L] = 2$ i $[L : \mathbb{Q}] = \varphi(k)/2$.

Recordem

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi les demostracions Euclidianes?

Recordem

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi les demostracions Euclidianes?

Implementarem el mètode general de Schur i veurem que obtenim una demostració Euclidiana i *elemental*.

Implementació pràctica

Recordem

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi les demostracions Euclidianes?

Implementarem el mètode general de Schur i veurem que obtenim una demostració Euclidiana i *elemental*.

LaTeX

Implementació pràctica

Recordem

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi les demostracions Euclidianes?

Implementarem el mètode general de Schur i veurem que obtenim una demostració Euclidiana i *elemental*.

LaTeX

Quan $\ell^2 \equiv 1 \pmod{k}$, generem qualsevol d'aquestes demostracions amb una pàgina web.

Implementació pràctica

Recordem

P2 Podem trobar un mètode *sistemàtic* i *elemental* que implementi les demostracions Euclidianes?

Implementarem el mètode general de Schur i veurem que obtenim una demostració Euclidiana i *elemental*.

LaTeX

Quan $\ell^2 \equiv 1 \pmod{k}$, generem qualsevol d'aquestes demostracions amb una pàgina web. Hem resolt finalment la pregunta P2.✓

Conclusions

- Hem demostrat de manera completa els teoremes de Schur i Murty.

Conclusions

- Hem demostrat de manera completa els teoremes de Schur i Murty.
- Donem un mètode sistemàtic per trobar demostracions Euclidianes de la infinitud de primers $\equiv \ell \pmod{k}$ quan $\ell^2 \equiv 1 \pmod{k}$.

Conclusions

- Hem demostrat de manera completa els teoremes de Schur i Murty.
- Donem un mètode sistemàtic per trobar demostracions Euclidianes de la infinitud de primers $\equiv \ell \pmod{k}$ quan $\ell^2 \equiv 1 \pmod{k}$.
- A més, implementem efectivament aquest mètode, de manera que les demostracions són elementals i accessibles per a tothom.

Conclusions

- Hem demostrat de manera completa els teoremes de Schur i Murty.
- Donem un mètode sistemàtic per trobar demostracions Euclidianes de la infinitud de primers $\equiv \ell \pmod{k}$ quan $\ell^2 \equiv 1 \pmod{k}$.
- A més, implementem efectivament aquest mètode, de manera que les demostracions són elementals i accessibles per a tothom.
- En el camí, hem donat una caracterització del conjunt $\mathrm{Spl}_1(L)$, per un cos L sota del ciclotòmic $\mathbb{Q}(\zeta)$ amb $[\mathbb{Q}(\zeta) : L] = 2$.

Referències I

K. Conrad.
Euclidean Proofs of Dirichlet's Theorem.
University of Connecticut, 2010.

M. Ram Murty and N. Thain.
Prime Numbers in certain Arithmetic Progressions.
Functiones et Approximatio Commentarii Mathematici, (XXXV): 249–259, 01 2008.

Gràcies!