

# Algebra és számelmélet

## ELTE Algebra és Számelmélet Tanszék

Konzultáció: Kiss Emil

<http://ewkiss.web.elte.hu/wp/wordpress>

[ewkiss@gmail.com](mailto:ewkiss@gmail.com)

27. előadás

# Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

# Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-osztóra.

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. Valóban, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

## Visszavezetés príमतvány-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  príमतvány-osztóra. Valóban, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$

# Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .



# Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. Valóban, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ ,

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ ,

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. Valóban, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható,

# Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. Valóban, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

Az  $\{x \equiv 0 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 28 \pmod{100}$ .

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

Az  $\{x \equiv 0 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 28 \pmod{100}$ .

Az  $\{x \equiv 0 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 72 \pmod{100}$ .

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

Az  $\{x \equiv 0 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 28 \pmod{100}$ .

Az  $\{x \equiv 0 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 72 \pmod{100}$ .

Az  $\{x \equiv 2 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 78 \pmod{100}$ .

## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

Az  $\{x \equiv 0 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 28 \pmod{100}$ .

Az  $\{x \equiv 0 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 72 \pmod{100}$ .

Az  $\{x \equiv 2 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 78 \pmod{100}$ .

Az  $\{x \equiv 2 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 22 \pmod{100}$ .



## Visszavezetés prímszám-modulusra

Az  $f(x) \equiv 0 \pmod{n}$  megoldásait keressük, ahol  $f \in \mathbb{Z}[x]$ .

Elegendő megoldani  $n$  prímszám-modulusra. **Valóban**, a kínai maradéktétel miatt ebből egyértelműen kapható megoldás mod  $n$ .

Mely négyzetszámok végződnek 84-re a tízes számrendszerben?

Ha  $x^2 \equiv 84 \pmod{100}$ , akkor  $x^2 \equiv 0 \pmod{4}$  és  $x^2 \equiv 9 \pmod{25}$ .

Az első kongruencia megoldásai  $x \equiv 0, 2 \pmod{4}$ .

A másodiké  $x \equiv \pm 3 \pmod{25}$ , hiszen ha  $25 \mid x^2 - 9 = (x - 3)(x + 3)$ , akkor valamelyik tényező 5-tel osztható, de mindkettő nem.

Az  $\{x \equiv 0 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 28 \pmod{100}$ .

Az  $\{x \equiv 0 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 72 \pmod{100}$ .

Az  $\{x \equiv 2 \pmod{4}, x \equiv 3 \pmod{25}\}$  megoldása  $x \equiv 78 \pmod{100}$ .

Az  $\{x \equiv 2 \pmod{4}, x \equiv -3 \pmod{25}\}$  megoldása  $x \equiv 22 \pmod{100}$ .

Ezért a 24-re, 28-ra, 72-re és 76-ra végződő számok a megfelelők.

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ ,

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ ,

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra.

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra.  
Az állításban  $f'$  az  $f$  deriváltját jelöli.

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.



# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

Áll.: Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt.

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ ,

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:  $a^m$

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:  $a^m$  és  $\binom{m}{1} a^{m-1} tp^j$ .  $\square$

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:  $a^m$  és  $\binom{m}{1} a^{m-1} tp^j$ .  $\square$

Legyen  $f(x) = a_0 + a_1 x + \dots + a_n x^n$ .

# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:  $a^m$  és  $\binom{m}{1} a^{m-1} tp^j$ .  $\square$

Legyen  $f(x) = a_0 + a_1x + \dots + a_nx^n$ . Az előző miatt

$f(a + tp^j) \equiv a_0 + a_1(a + tp^j) + \dots + a_n(a^n + tp^j n a^{n-1}) \pmod{p^{j+1}}$ .



# Visszavezetés prím modulusra

## Hensel-lemma (FGy3.7.1)

Legyen  $p$  prím. Tegyük föl, hogy  $f(c) \equiv 0 \pmod{p}$ .

Ha  $p \nmid f'(c)$ , akkor mod  $p^k$  egyértelműen létezik olyan  $c_k$  szám, melyre  $f(c_k) \equiv 0 \pmod{p^k}$ , és  $c_k \equiv c \pmod{p}$ .

Vagyis a megoldások egyértelműen „felemelhetők”  $p$ -ről  $p^k$ -ra. Az állításban  $f'$  az  $f$  deriváltját jelöli. A feltétel azt fejezi ki, hogy  $c$  egyszeres gyöke  $f$ -nek  $\mathbb{Z}_p$  fölött.

**Áll.:** Ha  $j \geq 1$ , akkor  $(a + tp^j)^m \equiv a^m + tp^j m a^{m-1} \pmod{p^{j+1}}$ .

**Biz:** Alkalmazzuk a binomiális tételt. Mivel  $p^{j+1} \mid (tp^j)^i$  ha  $i \geq 2$ , ezért mod  $p^{j+1}$  két tag marad:  $a^m$  és  $\binom{m}{1} a^{m-1} tp^j$ . □

Legyen  $f(x) = a_0 + a_1x + \dots + a_nx^n$ . Az előző miatt

$f(a + tp^j) \equiv a_0 + a_1(a + tp^j) + \dots + a_n(a^n + tp^j n a^{n-1}) \pmod{p^{j+1}}$ .

A jobb oldal  $f(a) + tp^j f'(a)$ . □

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

Bizonyítás  $k$  szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ ,

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban.

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ ,

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható,



# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ ),

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is),

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is), és akkor  $c_k$  felemelhető  $p$ -féleképpen,

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is), és akkor  $c_k$  felemelhető  $p$ -féleképpen, vagy egyáltalán nincs jó  $t$

## A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

### Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is), és akkor  $c_k$  felemelhető  $p$ -féleképpen, vagy egyáltalán nincs jó  $t$  (ha  $p^{k+1} \nmid f(c_k)$ ),

# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is), és akkor  $c_k$  felemelhető  $p$ -féleképpen, vagy egyáltalán nincs jó  $t$  (ha  $p^{k+1} \nmid f(c_k)$ ), és akkor  $c_k$  nem emelhető föl.



# A Hensel-lemma bizonyítása

Az  $f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$  összefüggést a FGy-könyv az analízisből ismeretes Taylor-formula segítségével igazolja.

## Bizonyítás $k$ szerinti indukcióval

Ha  $f(c_k) \equiv 0 \pmod{p^k}$  és  $c_k \equiv c \pmod{p}$ , akkor keressük  $c_{k+1}$ -et  $c_k + tp^k$  alakban. Ha  $0 \equiv f(c_k + tp^k) \equiv f(c_k) + tp^k f'(c_k) \pmod{p^{k+1}}$ , akkor  $p^k$ -val egyszerűsítve  $-f(c_k)/p^k \equiv t f'(c_k) \pmod{p}$  adódik (a bal oldalon egész szám áll, mert  $f(c_k) \equiv 0 \pmod{p^k}$ ).

Ez lineáris kongruencia  $t$ -re, ami egyértelműen megoldható, mert  $f'(c_k) \equiv f'(c) \pmod{p}$  nem osztható  $p$ -vel. □

Ha  $p \mid f'(c)$ , akkor az előző gondolatmenetben vagy minden  $t$  megfelelő (ha  $p^{k+1} \mid f(c_k)$ , azaz ha  $c_k$  már eleve megoldás mod  $p^{k+1}$  is), és akkor  $c_k$  felemelhető  $p$ -féleképpen, vagy egyáltalán nincs jó  $t$  (ha  $p^{k+1} \nmid f(c_k)$ ), és akkor  $c_k$  nem emelhető föl. Így  $p \mid f'(c)$  esetén a lemma nem dönti el, van-e megoldás mod  $p^{k+1}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük.

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  
 $x^2 \equiv 89 \equiv 4 \pmod{5}$ ,

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható. Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .



## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható. Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ . Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható. Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ . Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . **Ellenőrzés:**  $25 \mid 17^2 - 89 = 200$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . **Ellenőrzés:**  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .)

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .)

Az  $\{x \equiv 1 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 33 \pmod{100}$ .



## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .)

Az  $\{x \equiv 1 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 33 \pmod{100}$ .

Az  $\{x \equiv 1 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 17 \pmod{100}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .)

Az  $\{x \equiv 1 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 33 \pmod{100}$ .

Az  $\{x \equiv 1 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 17 \pmod{100}$ .

Az  $\{x \equiv 3 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 83 \pmod{100}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket.

Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható.

Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ .

Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ .

Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ .

Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ .

Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .)

Az  $\{x \equiv 1 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 33 \pmod{100}$ .

Az  $\{x \equiv 1 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 17 \pmod{100}$ .

Az  $\{x \equiv 3 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 83 \pmod{100}$ .

Az  $\{x \equiv 3 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 67 \pmod{100}$ .

## Példa a Hensel-lemma alkalmazására

Mely négyzetszámok végződnek 89-re a tízes számrendszerben?

$f(x) = x^2 - 89 \equiv 0 \pmod{25}$  megoldásait keressük. Mod 5 nézve  $x^2 \equiv 89 \equiv 4 \pmod{5}$ , a megoldások  $c \equiv \pm 2 \pmod{5}$ . Emeljük föl ezeket. Mivel  $(x^2 - 89)' = 2x$ , és  $2 \cdot (\pm 2) \not\equiv 0 \pmod{5}$ , a lemma alkalmazható. Ha  $c = 2$ , akkor  $4t \equiv (89 - 2^2)/5 \pmod{5}$  megoldása  $t \equiv 3 \pmod{5}$ . Ezért  $c_2 = 2 + 3 \cdot 5 = 17$ . Ellenőrzés:  $25 \mid 17^2 - 89 = 200$ . Ha  $c = -2$ , akkor  $-4t \equiv (89 - (-2)^2)/5 \pmod{5}$  megoldása  $t \equiv 2 \pmod{5}$ . Ezért  $c_2 = -2 + 2 \cdot 5 = 8$ . Ellenőrzés:  $25 \mid 8^2 - 89 = -25$ . Az  $x^2 \equiv 89 \equiv 1 \pmod{4}$  megoldásai nyilván  $x \equiv \pm 1 \pmod{4}$ . (A lemma most nem lenne alkalmazható, mert  $(x^2 - 89)' = 2x \equiv 0 \pmod{2}$ .) Az  $\{x \equiv 1 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 33 \pmod{100}$ . Az  $\{x \equiv 1 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 17 \pmod{100}$ . Az  $\{x \equiv 3 \pmod{4}, x \equiv 8 \pmod{25}\}$  megoldása  $x \equiv 83 \pmod{100}$ . Az  $\{x \equiv 3 \pmod{4}, x \equiv 17 \pmod{25}\}$  megoldása  $x \equiv 67 \pmod{100}$ . Tehát a 17, 33, 67, 83 végzések a jók.

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát,

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben.

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test,



# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test, ezért egy polinomnak legfeljebb annyi gyöke van, mint a foka.  $\square$

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test, ezért egy polinomnak legfeljebb annyi gyöke van, mint a foka.  $\square$

## Tétel (FGy3.1.3)

Ha a polinomban  $x^k$  helyett  $x^{k-p+1}$ -et írunk, akkor a mod  $p$  megoldások halmaza nem változik.

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test, ezért egy polinomnak legfeljebb annyi gyöke van, mint a foka.  $\square$

## Tétel (FGy3.1.3)

Ha a polinomban  $x^k$  helyett  $x^{k-p+1}$ -et írunk, akkor a mod  $p$  megoldások halmaza nem változik.

Továbbá  $x = 0$  vizsgálata után  $x^{p-1}$  helyébe is 1-et írhatunk.

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test, ezért egy polinomnak legfeljebb annyi gyöke van, mint a foka.  $\square$

## Tétel (FGy3.1.3)

Ha a polinomban  $x^k$  helyett  $x^{k-p+1}$ -et írunk, akkor a mod  $p$  megoldások halmaza nem változik.

Továbbá  $x = 0$  vizsgálata után  $x^{p-1}$  helyébe is 1-et írhatunk. Ezért elegendő  $p - 1$ -nél kisebb fokú polinomokat tekinteni.

# A megoldások maximális száma

## Tétel (FGy3.1.2)

Ha az  $f \in \mathbb{Z}[x]$  polinom mod  $p$  vett foka  $k$ , akkor az  $f(x) \equiv 0 \pmod{p}$  kongruenciának legfeljebb  $k$  megoldása van mod  $p$ .

Az  $f$  polinom mod  $p$  vett fokát úgy értjük, hogy vesszük a polinom együtthatóinak  $p$ -vel való osztási maradékát, és ennek fokát tekintjük  $\mathbb{Z}_p$ -ben. Az állítás következik abból, hogy  $\mathbb{Z}_p$  test, ezért egy polinomnak legfeljebb annyi gyöke van, mint a foka.  $\square$

## Tétel (FGy3.1.3)

Ha a polinomban  $x^k$  helyett  $x^{k-p+1}$ -et írunk, akkor a mod  $p$  megoldások halmaza nem változik.

Továbbá  $x = 0$  vizsgálata után  $x^{p-1}$  helyébe is 1-et írhatunk. Ezért elegendő  $p - 1$ -nél kisebb fokú polinomokat tekinteni.

Ez nyilvánvalóan következik a kis-Fermat-tételből.



# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$   
kongruencia megoldásszáma  $p - 1 - r$ ,

# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$  kongruencia megoldásszáma  $p - 1 - r$ , ahol  $r$  az alábbi mátrixnak

a  $\mathbb{Z}_p$  test fölötti rangja:

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$  kongruencia megoldásszáma  $p - 1 - r$ , ahol  $r$  az alábbi mátrixnak

a  $\mathbb{Z}_p$  test fölötti rangja:

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

Speciálisan akkor és csak akkor létezik megoldás, ha ennek a mátrixnak a determinánsa nulla mod  $p$ .



# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$  kongruencia megoldásszáma  $p - 1 - r$ , ahol  $r$  az alábbi mátrixnak

a  $\mathbb{Z}_p$  test fölötti rangja:

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

Speciálisan akkor és csak akkor létezik megoldás, ha ennek a mátrixnak a determinánsa nulla mod  $p$ .

Az utolsó állítás azért igaz, mert egy mátrix determinánsa akkor és csak akkor nulla, ha a rangja kisebb a méreténél

# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$  kongruencia megoldásszáma  $p - 1 - r$ , ahol  $r$  az alábbi mátrixnak

a  $\mathbb{Z}_p$  test fölötti rangja:

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

Speciálisan akkor és csak akkor létezik megoldás, ha ennek a mátrixnak a determinánsa nulla mod  $p$ .

Az utolsó állítás azért igaz, mert egy mátrix determinánsa akkor és csak akkor nulla, ha a rangja kisebb a méreténél (mert ilyenkor az oszlopok összefüggőek).

# A Kőnig–Rados-tétel

## Tétel (FGy3.6.2, NB)

Ha  $p \nmid a_0$ , akkor az  $f(x) = a_0 + a_1x + \dots + a_{p-2}x^{p-2} \equiv 0 \pmod{p}$  kongruencia megoldásszáma  $p - 1 - r$ , ahol  $r$  az alábbi mátrixnak

a  $\mathbb{Z}_p$  test fölötti rangja:

$$\begin{bmatrix} a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix}.$$

Speciálisan akkor és csak akkor létezik megoldás, ha ennek a mátrixnak a determinánsa nulla mod  $p$ .

Az utolsó állítás azért igaz, mert egy mátrix determinánsa akkor és csak akkor nulla, ha a rangja kisebb a méreténél (mert ilyenkor az oszlopok összefüggőek).

**HF:** Igazoljuk, hogy ha  $p$  prím, akkor  $x^2 \equiv -1 \pmod{p}$  pontosan akkor oldható meg, ha  $p \equiv 1 \pmod{4}$ .

# Mikor létezik primitív gyök?

Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ ,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod  $7$  a  $3$  és az  $5$ .

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1, 3^2 \equiv 2 \pmod{7}$ ,



# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.  
Modulo 9 a 2 és az 5 lesz primitív gyök.

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8,



# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ .

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ . Mod 15 sincs, mert ha  $(a, 15) = 1$ , akkor  $a^4 \equiv 1 \pmod{15}$ ,

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1$ ,  $3^2 \equiv 2 \pmod{7}$ ,  $3^3 \equiv 2 \cdot 3 = 6 \pmod{7}$ ,  $3^4 \equiv 2^2 = 4 \pmod{7}$ ,  
 $3^5 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$  és  $3^6 \equiv 1 \pmod{7}$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ . Mod 15 sincs, mert ha  $(a, 15) = 1$ , akkor  $a^4 \equiv 1 \pmod{15}$ , de  $\varphi(15) = 8$ .

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1, 3^2 \equiv 2 (7), 3^3 \equiv 2 \cdot 3 = 6 (7), 3^4 \equiv 2^2 = 4 (7), 3^5 \equiv 4 \cdot 3 \equiv 5 (7)$  és  $3^6 \equiv 1 (7)$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ . Mod 15 sincs, mert ha  $(a, 15) = 1$ , akkor  $a^4 \equiv 1 (15)$ , de  $\varphi(15) = 8$ .

## Tétel (FGy3.3.5)

Az  $m > 1$  modulusra pontosan akkor létezik primitív gyök, ha  $m = 2, 4,$

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1, 3^2 \equiv 2 (7), 3^3 \equiv 2 \cdot 3 = 6 (7), 3^4 \equiv 2^2 = 4 (7), 3^5 \equiv 4 \cdot 3 \equiv 5 (7)$  és  $3^6 \equiv 1 (7)$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ . Mod 15 sincs, mert ha  $(a, 15) = 1$ , akkor  $a^4 \equiv 1 (15)$ , de  $\varphi(15) = 8$ .

## Tétel (FGy3.3.5)

Az  $m > 1$  modulusra pontosan akkor létezik primitív gyök, ha  $m = 2, 4$ , egy páratlan prímszám, vagy  $m = 2p^k$ , ahol  $p$  páratlan prímszám,  $k \geq 1$ .

# Mikor létezik primitív gyök?

## Definíció (FGy3.3.1, 3.3.2)

A  $g$  szám primitív gyök mod  $m$ , ha rendje  $\varphi(m)$ , vagyis ha minden mod  $m$  redukált maradékosztályban van hatványa.

**Példák:** A primitív gyökök mod 7 a 3 és az 5.

Pl. 3-ra  $3^1, 3^2 \equiv 2 (7), 3^3 \equiv 2 \cdot 3 = 6 (7), 3^4 \equiv 2^2 = 4 (7), 3^5 \equiv 4 \cdot 3 \equiv 5 (7)$  és  $3^6 \equiv 1 (7)$  redukált maradékrendszer mod 7.

Modulo 9 a 2 és az 5 lesz primitív gyök.

Modulo 8 nincs, mert páratlan szám négyzete már 1-et ad maradékul mod 8, de  $\varphi(8) = 4$ . Mod 15 sincs, mert ha  $(a, 15) = 1$ , akkor  $a^4 \equiv 1 (15)$ , de  $\varphi(15) = 8$ .

## Tétel (FGy3.3.5)

Az  $m > 1$  modulusra pontosan akkor létezik primitív gyök, ha  $m = 2, 4$ , egy páratlan prímszám, vagy annak kétszerese.

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus esetén van primitív gyök.

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel.



# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  
 $T$  minden nem nulla eleme  $g$ -nek hatványa.

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  
 $T$  minden nem nulla eleme  $g$ -nek hatványa.

Az alábbi egy negyedik gondolatmenethez vezet,

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  
 $T$  minden nem nulla eleme  $g$ -nek hatványa.

Az alábbi egy negyedik gondolatmenethez vezet,  
az állítást később is felhasználjuk.

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  $T$  minden nem nulla eleme  $g$ -nek hatványa.

Az alábbi egy negyedik gondolatmenethez vezet, az állítást később is felhasználjuk.

## Tétel (K5.8.14)

Tegyük föl, hogy  $p$  prím, és  $p \nmid n$ .

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  $T$  minden nem nulla eleme  $g$ -nek hatványa.

Az alábbi egy negyedik gondolatmenethez vezet, az állítást később is felhasználjuk.

## Tétel (K5.8.14)

Tegyük föl, hogy  $p$  prím, és  $p \nmid n$ . Ekkor  $p \mid \Phi_n(c)$  akkor és csak akkor, ha  $o_p(c) = n$

# A prím modulus esete

## Tétel (FGy3.3.3)

Prím modulus estén van primitív gyök.

A Freud–Gyarmati-könyvben három bizonyítás is szerepel. Ezek egyikét módosítja a K4.3.22-beli gondolatmenet, ahol belátjuk:

ha  $T$  véges test, akkor van olyan  $g \neq 0 \in T$ , hogy  $T$  minden nem nulla eleme  $g$ -nek hatványa.

Az alábbi egy negyedik gondolatmenethez vezet, az állítást később is felhasználjuk.

## Tétel (K5.8.14)

Tegyük föl, hogy  $p$  prím, és  $p \nmid n$ . Ekkor  $p \mid \Phi_n(c)$  akkor és csak akkor, ha  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

# A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ ,



# A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek.

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is,



## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is.

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ .  
Ezzel beláttuk, hogy  $o_p(c) = n$ .



## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ .  
Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldálnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ .  
Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ ,  
akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is.

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött.  
Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ .  
Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is,  
és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  
 $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$   
és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  
 $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke  
a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ .  
Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ .  
Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ ,  
akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  
 $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ , tehát  $d = n$ . □

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ , tehát  $d = n$ . □

Korábban láttuk, hogy a kis Fermat-tétel miatt  $x^{p-1} - 1$  az összes olyan  $x - b$  gyöktényező szorzata, ahol  $0 \leq b < p$ .

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ , tehát  $d = n$ . □

Korábban láttuk, hogy a kis Fermat-tétel miatt  $x^{p-1} - 1$  az összes olyan  $x - b$  gyöktényező szorzata, ahol  $0 \leq b < p$ . Mivel  $x^{p-1} - 1 = \prod_{d|p-1} \Phi_d(x)$ ,

## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ , tehát  $d = n$ . □

Korábban láttuk, hogy a kis Fermat-tétel miatt  $x^{p-1} - 1$  az összes olyan  $x - b$  gyöktényező szorzata, ahol  $0 \leq b < p$ . Mivel  $x^{p-1} - 1 = \prod_{d|p-1} \Phi_d(x)$ , ezért  $\Phi_{p-1}$  is gyöktényezőkre bomlik  $\mathbb{Z}_p$ -ben,



## A tétel bizonyítása

Tudjuk, hogy  $\prod_{d|n} \Phi_d(x) = x^n - 1$ , ezt nézzük  $\mathbb{Z}_p$  fölött. Mivel  $c$  gyöke a baloldalnak, ezért  $c^n \equiv 1 \pmod{p}$ , azaz  $o_p(c) \mid n$ . Tegyük föl, hogy  $k = o_p(c) < n$ . Ekkor  $c$  gyöke  $x^k - 1$ -nek is, és mivel  $x^k - 1 = \prod_{d|k} \Phi_d(x)$ , van olyan  $d \mid k$ , hogy  $c$  gyöke  $\Phi_d(x)$ -nek. De akkor az  $x - c$  gyöktényező kiemelhető a  $\Phi_d(x)$  és a  $\Phi_n(x)$  polinomokból is, ezért  $(x - c)^2 \mid x^n - 1$ . Vagyis  $c$  legalább kétszeres gyöke  $x^n - 1$ -nek  $\mathbb{Z}_p$  fölött, és ezért gyöke a deriváltjának is. De  $(x^n - 1)' = nx^{n-1}$ , azaz  $nc^{n-1} \equiv 0 \pmod{p}$ . Mivel  $p \nmid n$ , ezért  $p \mid c$ , ami ellentmond annak, hogy  $c^n \equiv 1 \pmod{p}$ . Ezzel beláttuk, hogy  $o_p(c) = n$ . **Megfordítva**, ha  $o_p(c) = n$ , akkor  $c$  gyöke  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ -nek, tehát valamelyik  $\Phi_d$ -nek is. De  $\Phi_d(x) \mid x^d - 1$ , tehát  $d = n$ . □

Korábban láttuk, hogy a kis Fermat-tétel miatt  $x^{p-1} - 1$  az összes olyan  $x - b$  gyöktényező szorzata, ahol  $0 \leq b < p$ . Mivel  $x^{p-1} - 1 = \prod_{d|p-1} \Phi_d(x)$ , ezért  $\Phi_{p-1}$  is gyöktényezőkre bomlik  $\mathbb{Z}_p$ -ben, és **minden gyöke primitív gyök mod  $p$** .

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet.

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”,

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ .

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll,

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben.

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p-1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ .



# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p-1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .  
A  $d$  rendű elemek száma  $d \mid \varphi(m)$  esetén  $\varphi(d)$ ,

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p-1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .  
A  $d$  rendű elemek száma  $d \mid \varphi(m)$  esetén  $\varphi(d)$ , ezek a  $g^k$  alakú elemek, ahol  $(k, \varphi(m)) = \varphi(m)/d$ .

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p-1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .  
A  $d$  rendű elemek száma  $d \mid \varphi(m)$  esetén  $\varphi(d)$ , ezek a  $g^k$  alakú elemek, ahol  $(k, \varphi(m)) = \varphi(m)/d$ .

Mindez a hatvány rendjének képletéből következik,

# Egységgyökök mod $p$

Érdemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p-1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .  
A  $d$  rendű elemek száma  $d \mid \varphi(m)$  esetén  $\varphi(d)$ , ezek a  $g^k$  alakú elemek, ahol  $(k, \varphi(m)) = \varphi(m)/d$ .

Mindez a hatvány rendjének képletéből következik, ahogy az analóg állítás komplex számok esetében is,

# Egységgyökök mod $p$

Érdeemes egy analógiára felhívni a figyelmet. A  $\mathbb{Z}_p$  testben az Euler–Fermat-tétel miatt minden  $b \neq 0$  elem „ $p - 1$ -edik egységgyök”, hiszen  $b^{p-1} \equiv 1 \pmod{p}$ . A „primitív” kifejezés azt jelenti, hogy egy ilyen hatványaiként az összes többi egységgyök előáll, mind  $\mathbb{C}$ -ben, mind  $\mathbb{Z}_p$ -ben. Az előző bizonyítás mutatja, milyen szoros kapcsolat van a két fogalom között.

## Tétel (FGy3.3.4, K4.3.24)

Ha  $g$  primitív gyök mod  $m$ , akkor  $g^k$  pontosan akkor primitív gyök, ha  $(k, \varphi(m)) = 1$ . Ezért számuk  $\varphi(\varphi(m))$ .  
A  $d$  rendű elemek száma  $d \mid \varphi(m)$  esetén  $\varphi(d)$ , ezek a  $g^k$  alakú elemek, ahol  $(k, \varphi(m)) = \varphi(m)/d$ .

Mindez a hatvány rendjének képletéből következik, ahogy az analóg állítás komplex számok esetében is, mert valójában csoportelméleti tételről van szó.



# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

Valóban, legyen  $m = o_{p^k}(g)$ .



primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

Valóban, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz,

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ .

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt.

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ ,

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_p(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ ,

primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ ,



primitív gyök mod  $p^2$  \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ .

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2}$

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$ ,

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$ , ami nem kongruens 1-gyel mod  $p^2$ ,

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$ , ami nem kongruens 1-gyel mod  $p^2$ , hiszen  $p \nmid g$ .

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$ , ami nem kongruens 1-gyel mod  $p^2$ , hiszen  $p \nmid g$ . Ezért  $o_{p^2}(g+p)$  nem  $p-1$ ,

# primitív gyök mod $p^2$ \*

Legyen  $p$  páratlan prím, PGY=primitív gyök.

Ha  $g$  PGY mod  $p$ , akkor  $o_{p^k}(g) = p^\ell(p-1)$ , ahol  $0 \leq \ell < p$ .

**Valóban**, legyen  $m = o_{p^k}(g)$ . Ekkor  $g^m \equiv 1 \pmod{p}$  is igaz, ezért  $p-1 = o_p(g) \mid m$ . De  $m \mid \varphi(p^k) = p^{k-1}(p-1)$  az Euler–Fermat miatt. Ezért  $m/(p-1) \mid p^{k-1}$ , tehát  $p^\ell$  ahol  $0 \leq \ell < p$ .  $\square$

## Tétel (FGy3.3.5/L1)

Ha  $g$  PGY mod  $p$ , akkor  $g$  vagy  $g+p$  PGY mod  $p^2$ .

Tegyük föl, hogy  $g$  nem PGY mod  $p^2$ , ekkor az előző állítás miatt  $o_{p^2}(g) = p-1$ , így  $g^{p-1} \equiv 1 \pmod{p^2}$ . A Hensel-lemma szerint  $(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \pmod{p^2}$ , ami nem kongruens 1-gyel mod  $p^2$ , hiszen  $p \nmid g$ . Ezért  $o_{p^2}(g+p)$  nem  $p-1$ , és így az előző állítás miatt  $p(p-1)$ .  $\square$

primitív gyök mod  $p^k$  \*

Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).



primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p - 1)$ .

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ ,

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ ,

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ ,



primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + tp^j m a^{m-1} (p^{j+2})$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ .

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + tp^j m a^{m-1} (p^{j+2})$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ . Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ . A fenti képlet szerint  $1 \equiv g^{p(p-1)} = (1 + tp)^p \equiv 1 + tp^2 \pmod{p^3}$ ,

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + tp^j m a^{m-1} (p^{j+2})$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ . A fenti képlet szerint  $1 \equiv g^{p(p-1)} = (1 + tp)^p \equiv 1 + tp^2 \pmod{p^3}$ , ahonnan  $p \mid t$ .

# primitív gyök mod $p^k$ \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + tp^j ma^{m-1} \pmod{p^{j+2}}$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ . A fenti képlet szerint  $1 \equiv g^{p(p-1)} = (1 + tp)^p \equiv 1 + tp^2 \pmod{p^3}$ , ahonnan  $p \mid t$ . Így  $g^{p-1} \equiv 1 \pmod{p^2}$ ,

primitív gyök mod  $p^k$  \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + tp^j m a^{m-1} (p^{j+2})$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ . A fenti képlet szerint  $1 \equiv g^{p(p-1)} = (1 + tp)^p \equiv 1 + tp^2 \pmod{p^3}$ , ahonnan  $p \mid t$ . Így  $g^{p-1} \equiv 1 \pmod{p^2}$ , ez ellentmond annak, hogy  $g$  PGY mod  $p^2$ . □

# primitív gyök mod $p^k$ \*

## Tétel (FGy3.3.5/L2)

Ha  $g$  PGy mod  $p^2$ , akkor  $g$  PGY mod  $p^k$  ( $k \geq 3$ ).

Bizonyítás a Freud–Gyarmati-könyvben, itt csak  $k = 3$ -ra igazoljuk.

## A Hensel-lemma bizonyításához hasonlóan:

Ha  $p \geq 3$ , továbbá vagy  $j \geq 2$ , vagy  $j \geq 1$  és  $p \mid m$ , akkor  $(a + p^j t)^m \equiv a^m + t p^j m a^{m-1} (p^{j+2})$ . □

Láttuk:  $o_{p^3}(g) = p^\ell(p-1)$ . Mivel  $g$  PGY mod  $p^2$ , ezért  $\ell \geq 1$ , és ha nem PGY mod  $p^3$ , akkor  $\ell \leq 1$ , így  $o_{p^3}(g) = p(p-1)$ .

Tudjuk, hogy  $g^{p-1} \equiv 1 \pmod{p}$ , ezért  $g^{p-1} = 1 + tp$ . A fenti képlet szerint  $1 \equiv g^{p(p-1)} = (1 + tp)^p \equiv 1 + tp^2 \pmod{p^3}$ , ahonnan  $p \mid t$ .

Így  $g^{p-1} \equiv 1 \pmod{p^2}$ , ez ellentmond annak, hogy  $g$  PGY mod  $p^2$ . □

**HF:** Ha  $p^k \mid b-1$ , de  $p^{k+1} \nmid b-1$ , akkor  $p^{k+2} \nmid b^p - 1$ .

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ .

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)



# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ ,

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ ,  
így mod  $2p^k$  is.

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ ,  
így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ .

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ . Ekkor  $t > 1$

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ . Ekkor  $t > 1$  és  $t^2 = 1 + 2 \cdot 2^{k-1} + 2^{2k} \equiv 1 \pmod{2^k}$ .



# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ . Ekkor  $t > 1$  és  $t^2 = 1 + 2 \cdot 2^{k-1} + 2^{2k} \equiv 1 \pmod{2^k}$ . Így  $t > 1$  miatt ez két másodrendű elem.

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímszám, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ . Ekkor  $t > 1$  és  $t^2 = 1 + 2 \cdot 2^{k-1} + 2^{2k} \equiv 1 \pmod{2^k}$ . Így  $t > 1$  miatt ez két másodrendű elem. De láttuk korábban, hogy ha van PGY mod  $m$ , akkor pontosan  $\varphi(2) = 1$  darab másodrendű elem van mod  $m$ .

# Primitív gyök mod $m$

## Tétel (FGy3.3.5/L3)

Ha  $g$  PGY mod  $p^k$ , akkor  $g$  és  $g + p^k$  közül a páratlan PGY mod  $2p^k$ . (A páratlant kell venni, hogy relatív prím legyen  $2p^k$ -hoz.)

Mindkettőnek  $\varphi(p^k)$  különböző hatványa van mod  $p^k$ , így mod  $2p^k$  is. De  $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$ . □

## Tétel (K4.9.10, a csoportelmélet során igazoljuk)

Ha mod  $m$  van PGY, akkor  $m$  prímhatvány, vagy annak kétszerese.

Végül legyen  $m = 2^k$ , ahol  $k \geq 3$  és  $t = 2^{k-1} \pm 1 > 1$ . Ekkor  $t > 1$  és  $t^2 = 1 + 2 \cdot 2^{k-1} + 2^{2k} \equiv 1 \pmod{2^k}$ . Így  $t > 1$  miatt ez két másodrendű elem. De láttuk korábban, hogy ha van PGY mod  $m$ , akkor pontosan  $\varphi(2) = 1$  darab másodrendű elem van mod  $m$ . Ezért nincs PGY mod  $2^k$ , ha  $k \geq 3$ .

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ .



# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú. Ha minden prímosztója  $4k + 1$  alakú lenne, akkor a szorzat is  $4k + 1$  alakú lenne,

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú. Ha minden prímosztója  $4k + 1$  alakú lenne, akkor a szorzat is  $4k + 1$  alakú lenne, ami lehetetlen.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú. Ha minden prímosztója  $4k + 1$  alakú lenne, akkor a szorzat is  $4k + 1$  alakú lenne, ami lehetetlen. Ezért van egy  $p \mid N$ , ami  $4k - 1$  alakú.

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú. Ha minden prímosztója  $4k + 1$  alakú lenne, akkor a szorzat is  $4k + 1$  alakú lenne, ami lehetetlen. Ezért van egy  $p \mid N$ , ami  $4k - 1$  alakú. Ez különbözik mindegyik  $p_i$ -től,

# Dirichlet tétele

## Dirichlet tétele (FGy5.3.1)

Ha  $(a, b) = 1$ , akkor az  $ak + b$  ( $k \geq 1$ ) számtani sorozatban végtelen sok prímszám van.

A feltétel nyilván szükséges, hiszen  $(a, b)$  osztja a sorozat minden tagját. A bizonyítás nehéz, a komplex analízis eszköztárát igényli.

## Speciális eset (FGy5.3.2)

Végtelen sok  $4k - 1$  alakú prím van.

Valóban, tegyük föl, hogy csak véges sok van, ezek  $p_1, p_2, \dots, p_k$ . Tekintsük a  $N = 4p_1 \dots p_k - 1 > 1$  számot. Ez  $4k - 1$  alakú. Ha minden prímosztója  $4k + 1$  alakú lenne, akkor a szorzat is  $4k + 1$  alakú lenne, ami lehetetlen. Ezért van egy  $p \mid N$ , ami  $4k - 1$  alakú. Ez különbözik mindegyik  $p_i$ -től, mert különben  $p \mid N$  és  $p \mid p_1, p_2, \dots, p_k$  miatt  $p \mid -1$  teljesülne.



Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.



Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ ,

Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$

Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van, ezek  $p_1, p_2, \dots, p_k$ .

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van, ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van, ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész. Tekintsük a  $N = \Phi_n(c)$  számot,

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ ,



Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ ,

Az  $nk + 1$  eset

Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ ,

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik.

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú.

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím

tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ ,

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1 p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ , ezért  $p \neq p_i$ .

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ , ezért  $p \neq p_i$ .

Be kell még látni, hogy  $N$ -nek van prímosztója,



Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ , ezért  $p \neq p_i$ .

Be kell még látni, hogy  $N$ -nek van prímosztója, vagyis  $N \neq \pm 1$ .

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ , ezért  $p \neq p_i$ .

Be kell még látni, hogy  $N$ -nek van prímosztója, vagyis  $N \neq \pm 1$ .

De a  $\Phi_n(np_1p_2 \dots p_k x)$  polinom minden értéket csak véges sok helyen vehet föl,

Az  $nk + 1$  eset

## Tétel (FGy5.3.4, K5.8.15)

Végtelen sok  $nk + 1$  alakú prím van.

Korábban már láttuk, hogy ha  $p$  prím,  $p \nmid n$ , és  $p \mid \Phi_n(c)$ , akkor  $o_p(c) = n$  (itt  $\Phi_n$  az  $n$ -edik körosztási polinom).

Tegyük föl, hogy csak véges sok  $nk + 1$  alakú prím van,

ezek  $p_1, p_2, \dots, p_k$ . Legyen  $c = np_1p_2 \dots p_k M$ , ahol  $M$  egész.

Tekintsük a  $N = \Phi_n(c)$  számot, és legyen  $p$  ennek prímosztója.

Tudjuk, hogy  $\Phi_n(x) \mid x^n - 1$ , ezért  $p \mid N \mid c^n - 1$ .

Mivel  $n \mid c$ , ezért  $p \nmid n$ , és így a fent idézett állítás szerint

$o_p(c) = n$ , amiből  $n \mid \varphi(p) = p - 1$  következik. Tehát a  $p$  prím tényleg  $nk + 1$  alakú. Mivel  $p_i \mid c$  és  $p \mid c^n - 1$ , ezért  $p \neq p_i$ .

Be kell még látni, hogy  $N$ -nek van prímosztója, vagyis  $N \neq \pm 1$ .

De a  $\Phi_n(np_1p_2 \dots p_k x)$  polinom minden értéket csak véges sok helyen vehet föl, így  $\Phi_n(np_1p_2 \dots p_k M) \neq \pm 1$  alkalmas  $M$ -re.  $\square$

# A 27. előadáshoz tartozó vizsgaanyag

## Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma,

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímszámra, illetve prímszámra,  
Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma,  
a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).



## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prímm modulusra van primitív gyök (FGy3.3.3, K4.3.22),

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prím modulusra van primitív gyök (FGy3.3.3, K4.3.22),

kapcsolat a körosztási polinom értékeinek prímosztóival (K5.8.14).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prím modulusra van primitív gyök (FGy3.3.3, K4.3.22),

kapcsolat a körosztási polinom értékeinek prímosztóival (K5.8.14).

A számok rendje mod  $p$  (FGy3.3.4, K4.3.24).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prím modulusra van primitív gyök (FGy3.3.3, K4.3.22),

kapcsolat a körosztási polinom értékeinek prímosztóival (K5.8.14).

A számok rendje mod  $p$  (FGy3.3.4, K4.3.24).

Mod  $p$  primitív gyök fölemelése mod  $p^k$  primitív gyökké (FGy3.3.5, NB).

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prím modulusra van primitív gyök (FGy3.3.3, K4.3.22),

kapcsolat a körosztási polinom értékeinek prímosztóival (K5.8.14).

A számok rendje mod  $p$  (FGy3.3.4, K4.3.24).

Mod  $p$  primitív gyök fölemelése mod  $p^k$  primitív gyökké (FGy3.3.5, NB). Dirichlet tétele (NB),

## A 27. előadáshoz tartozó vizsgaanyag

### Fogalmak

Primitív gyök mod  $m$  (FGy3.3.1–2).

### Tételek

Kongruencia visszavezetése prímmhatvány, illetve prímm modulusra, Hensel-lemma (FGy3.7.1). A mod  $p$  megoldások száma, a Kőnig–Rados-tétel (FGy3.1.2–3, FGY3.6.2, NB).

Mely modulusokra van primitív gyök (FGy3.3.5, K4.9.10).

Prím modulusra van primitív gyök (FGy3.3.3, K4.3.22),

kapcsolat a körosztási polinom értékeinek prímosztóival (K5.8.14).

A számok rendje mod  $p$  (FGy3.3.4, K4.3.24).

Mod  $p$  primitív gyök fölemelése mod  $p^k$  primitív gyökké (FGy3.3.5, NB). Dirichlet tétele (NB), a  $4k + 1$  és  $nk + 1$  eset (FGy5.3.1–2, 5.3.4, K5.8.15).