

Algebra és számelmélet

ELTE Algebra és Számelmélet Tanszék

Konzultáció: Kiss Emil

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

ewwkiss@gmail.com

28. előadás

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p .

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** ,

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$,

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek,

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi. Mindez elmondható minden olyan m modulusra, amire nézve van primitív gyök.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi. Mindez elmondható minden olyan m modulusra, amire nézve van primitív gyök. Ekkor $p - 1$ helyett $\varphi(m)$ szerepel.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi.

Mindez elmondható minden olyan m modulusra, amire nézve van primitív gyök. Ekkor $p - 1$ helyett $\varphi(m)$ szerepel.

A diszkrét logaritmust néha **indexnek** is hívják.

Diszkrét logaritmus

Definíció (FGy3.4.1)

Legyen p rögzített prím és g primitív gyök mod p . Ha $(a, p) = 1$, akkor van olyan $0 \leq k \leq p - 2$, hogy $g^k \equiv a \pmod{p}$. Ennek neve az a **diszkrét logaritmusa mod g** , jele $\log_{g,p}(a)$.

Mivel $o_p(g) = p - 1$, ezért $g^k \equiv g^\ell \pmod{p}$ akkor és csak akkor, ha $k - \ell$ jó kitevője g -nek, azaz ha $k \equiv \ell \pmod{p - 1}$. Ezért a diszkrét logaritmus mod $p - 1$ lesz egyértelmű. A rá vonatkozó azonosságok ugyanazok, mint a közönséges logaritmuséi.

Mindez elmondható minden olyan m modulusra, amire nézve van primitív gyök. Ekkor $p - 1$ helyett $\varphi(m)$ szerepel.

A diszkrét logaritmust néha **indexnek** is hívják.

Példa

Ha $p = 7$, akkor $\log_{3,7}(4) = 4$ és $\log_{3,7}(5) = 5$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.
Ilyenkor a mod p megoldások száma $(k, p-1)$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$,

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$,

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ binom kongruencia pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$,

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k, p-1)$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k, p-1)$.

Egy b pontosan akkor megoldás, ha g^b megoldása az eredeti kongruenciának,

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k, p-1)$.

Egy b pontosan akkor megoldás, ha g^b megoldása az eredeti kongruenciának, tehát $x^k \equiv a \pmod{p}$ megoldásszáma is $(k, p-1)$.

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k, p-1)$.

Egy b pontosan akkor megoldás, ha g^b megoldása az eredeti kongruenciának, tehát $x^k \equiv a \pmod{p}$ megoldásszáma is $(k, p-1)$.

Végül $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$ azzal ekvivalens, hogy

$m(p-1)/(k, p-1)$ jó kitevője g -nek,

Binom kongruenciák

Tétel (FGy3.5.1)

Legyen p prím és $(a, p) = 1$. Az $x^k \equiv a \pmod{p}$ **binom kongruencia** pontosan akkor oldható meg, ha $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$.

Ilyenkor a mod p megoldások száma $(k, p-1)$.

A megoldhatóság azzal ekvivalens, hogy $(k, p-1) \mid \log_{g,p}(a)$.

Diszkrét logaritmust használunk. Legyen g primitív gyök mod p , és $a \equiv g^m \pmod{p}$, azaz $m = \log_{g,p}(a)$, továbbá $y = \log_{g,p}(x)$.

Ekkor $(g^y)^k \equiv g^m \pmod{p}$ azzal ekvivalens, hogy $yk \equiv m \pmod{p-1}$.

Ez a lineáris kongruencia akkor oldható meg, ha $(k, p-1) \mid m$, és ilyenkor a mod $p-1$ megoldások száma $(k, p-1)$.

Egy b pontosan akkor megoldás, ha g^b megoldása az eredeti kongruenciának, tehát $x^k \equiv a \pmod{p}$ megoldásszáma is $(k, p-1)$.

Végül $a^{(p-1)/(k, p-1)} \equiv 1 \pmod{p}$ azzal ekvivalens, hogy

$m(p-1)/(k, p-1)$ jó kitevője g -nek, azaz $p-1$ -gyel osztható. □

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p ,

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak.

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$.

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**.

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -edik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámolás van.)

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -edik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámolás van.)

Az a akkor lesz k -edik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható.

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -edik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámolás van.)

Az a akkor lesz k -edik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -edik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható.

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -edik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámolás van.)

Az a akkor lesz k -edik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -edik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$.

Hatványmaradékok

Ha p prím, akkor a k -edik **hatványmaradékok** a teljes k -edik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -edik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámolás van.)

Az a akkor lesz k -edik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -edik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -edik hatványmaradékok halmaza,

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg.

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$,

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$, ahol c^{-1} a b inverze mod p .

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$, ahol c^{-1} a b inverze mod p (amelyre $bc^{-1} \equiv 1 \pmod{p}$).

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$, ahol c^{-1} a b inverze mod p (amelyre $bc^{-1} \equiv 1 \pmod{p}$). Így $b \equiv ca \pmod{p}$.

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$, ahol c^{-1} a b inverze mod p (amelyre $bc^{-1} \equiv 1 \pmod{p}$). Így $b \equiv ca \pmod{p}$. Az előző tétel szerint ilyen a -ból $(k, p-1)$ van,

Hatványmaradékok

Ha p prím, akkor a k -adik **hatványmaradékok** a teljes k -adik hatványok maradékai mod p , de a nullát nem tekintjük hatványmaradéknak. Számuk $(p-1)/(k, p-1)$. A többi nem nulla mod p maradék neve: k -adik **hatvány-nemmaradék**. (FGy3.5.2–3-ban egy alternatív leszámlálás van.)

Az a akkor lesz k -adik hatványmaradék, ha $x^k \equiv a \pmod{p}$ megoldható. Az előző tétel szerint a k -adik hatványmaradékok azok, amelyek indexe $(k, p-1)$ -gyel osztható. Tekintsük az $x \mapsto x^k \pmod{p}$ függvényt, ahol $(x, p) = 1$. Ennek képe a k -adik hatványmaradékok halmaza, ezért elég megmutatni, hogy mindegyiket $(k, p-1)$ -szer kapjuk meg. Ha $d = c^k$, akkor $b^k \equiv d = c^k \pmod{p}$ akkor és csak akkor, ha $a = bc^{-1}$ -re $a^k \equiv 1 \pmod{p}$, ahol c^{-1} a b inverze mod p (amelyre $bc^{-1} \equiv 1 \pmod{p}$). Így $b \equiv ca \pmod{p}$. Az előző tétel szerint ilyen a -ból $(k, p-1)$ van, tehát adott c -hez tényleg $(k, p-1)$ megfelelő b tartozik. □

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem. A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem. A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$. Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$,

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1 \pmod{p}$.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1 \pmod{p}$.

A kis Fermat-tétel miatt $a^{p-1} \equiv 1 \pmod{p}$,

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1 \pmod{p}$.

A kis Fermat-tétel miatt $a^{p-1} \equiv 1 \pmod{p}$, ezért $x = a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem.

A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$.

Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1 \pmod{p}$.

A kis Fermat-tétel miatt $a^{p-1} \equiv 1 \pmod{p}$, ezért $x = a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Az előző tétel miatt $a^{(p-1)/2} \equiv 1 \pmod{p}$ ha a kvadratikus maradék,

Euler-lemma

Definíció (Fgy4.1.1)

A **kvadratikus maradékok** és nemmaradékok a k -adik hatványmaradékok, illetve nemmaradékok, amikor $k = 2$.

Legyen a p prím páratlan. Az előző tétel speciális esete a következő.

Euler-lemma (FGy4.1.2)

Ha $(a, p) = 1$, akkor $a^{(p-1)/2}$ aszerint kongruens 1 -gyel vagy -1 -gyel mod p , hogy a kvadratikus maradék-e vagy sem. A kvadratikus maradékok és nemmaradékok száma is $(p-1)/2$. Ha a kvadratikus maradék, akkor $x^2 \equiv a \pmod{p}$ -nek 2 megoldása van.

Ha $x^2 \equiv 1 \pmod{p}$, akkor $p \mid x^2 - 1 = (x-1)(x+1)$, így $x \equiv \pm 1 \pmod{p}$. A kis Fermat-tétel miatt $a^{p-1} \equiv 1 \pmod{p}$, ezért $x = a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Az előző tétel miatt $a^{(p-1)/2} \equiv 1 \pmod{p}$ ha a kvadratikus maradék, ezért a $(p-1)/2$ nemmaradék esetében -1 -et kapunk mod p .

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem,
és 0 , ha $p \mid a$.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem,
és 0 , ha $p \mid a$. Ez a **Legendre szimbólum**

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

(3) A -1 a $4k + 1$ alakú prímekre lesz kvadratikus maradék. \square

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

(3) A -1 a $4k + 1$ alakú prímekre lesz kvadratikus maradék. \square

HF: Vezessük le a Wilson-tételből is, hogy -1 kvadratikus maradék a $4k + 1$ alakú prímekre.

Legendre-szimbólum

Definíció (FGy4.1.3)

Legyen $\left(\frac{a}{p}\right) = 1$, ha a kvadratikus maradék mod p , -1 ha nem, és 0 , ha $p \mid a$. Ez a **Legendre szimbólum** (p páratlan prím).

Az Euler-lemma szerint $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. Így igaz a következő.

Tétel (FGy4.1.4)

Tegyük fel, hogy p páratlan prím.

(1) Ha $a \equiv b \pmod{p}$, akkor $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

(3) A -1 a $4k + 1$ alakú prímeke lesz kvadratikus maradék. \square

HF: Vezessük le a Wilson-tételből is, hogy -1 kvadratikus maradék a $4k + 1$ alakú prímeke. **Ötlet:** A $(p - 1)!$ szorzatban párosítsunk minden számot az ellentettjével.

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p ,

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá,

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá, az egyik a Freud–Gyarmati-könyvben olvasható.

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá, az egyik a Freud–Gyarmati-könyvben olvasható. Mi egy későbbi kurzus keretében egy elegáns bizonyítást fogunk látni,

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá, az egyik a Freud–Gyarmati-könyvben olvasható. Mi egy későbbi kurzus keretében egy elegáns bizonyítást fogunk látni, amely **Gauss-összegeken**,

Kvadratikus reciprocitás

Tétel (Gauss, lásd FGy4.2.3), NB

Ha $p \neq q$ páratlan prímelek, akkor
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Tétel (FGy4.2.2, NB)

Ha p páratlan prím, akkor
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Azaz 2 akkor lesz kvadratikus maradék mod p , ha $p \equiv \pm 1 \pmod{8}$.

A reciprocitási tétel nehéz, Gauss maga nyolc különböző bizonyítást adott rá, az egyik a Freud–Gyarmati-könyvben olvasható. Mi egy későbbi kurzus keretében egy elegáns bizonyítást fogunk látni, amely **Gauss-összegeken**, és a **véges testek** tulajdonságain alapszik.

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\left(\frac{38}{79}\right) =$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\left(\frac{38}{79}\right) = \left(\frac{2}{79}\right) \left(\frac{19}{79}\right)$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\left(\frac{38}{79}\right) = \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) =$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\left(\frac{38}{79}\right) = \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) =$$

$$79 \equiv 3 \pmod{19}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) \\ 79 &\equiv 3 \pmod{19} \end{aligned}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) \end{aligned}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) \\ 19 &\equiv 1 \pmod{3} \end{aligned}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) \\ 19 &\equiv 1 \pmod{3} \end{aligned}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható.

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14 \pmod{79}$,

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14 \pmod{79}$, de a megoldást a fenti eljárás nem adja meg.

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14 \pmod{79}$, de a megoldást a fenti eljárás nem adja meg.

Probléma: Fel tudjuk-e a „számlálót” prímeekre bontani?

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14 \pmod{79}$, de a megoldást a fenti eljárás nem adja meg.

Probléma: Fel tudjuk-e a „számlálót” prímekre bontani?

Definíció (FGy4.3.1)

Ha az $m > 1$ páratlan szám a nem feltétlenül különböző p_1, \dots, p_k prímek szorzata, akkor legyen $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \dots \cdot \left(\frac{a}{p_k}\right)$.

Ez a kiterjesztés a **Jacobi-szimbólum**,

Példa a reciprocitási tétel használatára

Megoldható-e az $x^2 \equiv 38 \pmod{79}$ kongruencia?

$$\begin{aligned} \left(\frac{38}{79}\right) &= \left(\frac{2}{79}\right) \left(\frac{19}{79}\right) = (-1)^{\frac{79^2-1}{8}} (-1)^{\frac{19-1}{2} \frac{79-1}{2}} \left(\frac{79}{19}\right) = \\ &= 1 \cdot (-1) \cdot \left(\frac{3}{19}\right) = -(-1)^{\frac{3-1}{2} \frac{19-1}{2}} \left(\frac{19}{3}\right) = -(-1) \cdot \left(\frac{1}{3}\right) = 1. \end{aligned}$$

Ezért a kongruencia megoldható. Az eredmény $x \equiv \pm 14 \pmod{79}$, de a megoldást a fenti eljárás nem adja meg.

Probléma: Fel tudjuk-e a „számlálót” prímekekre bontani?

Definíció (FGy4.3.1)

Ha az $m > 1$ páratlan szám a nem feltétlenül különböző p_1, \dots, p_k prímekek szorzata, akkor legyen $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdot \dots \cdot \left(\frac{a}{p_k}\right)$.

Ez a kiterjesztés a **Jacobi-szimbólum**, segít a faktorizáció-problémán.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

(1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

(1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

(2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

$$(1) \text{ Ha } a \equiv b \pmod{m}, \text{ akkor } \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

$$(2) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right) \text{ és } \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right).$$

$$(3) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$$

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

$$(1) \text{ Ha } a \equiv b \pmod{m}, \text{ akkor } \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

$$(2) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right) \text{ és } \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right).$$

$$(3) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \text{ és } \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

$$(1) \text{ Ha } a \equiv b \pmod{m}, \text{ akkor } \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

$$(2) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right) \text{ és } \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right).$$

$$(3) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \text{ és } \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

$$(4) \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right)$$

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

- (1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
- (2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.
- (3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ és $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
- (4) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right)$ (ha $(m, n) \neq 1$, akkor mindkettő 0).

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

- (1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
- (2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.
- (3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ és $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
- (4) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right)$ (ha $(m, n) \neq 1$, akkor mindkettő 0).

E szabályok formálisan, azonnal következnek a Legendre-szimbólum tulajdonságaiból.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

- (1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
- (2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.
- (3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ és $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
- (4) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right)$ (ha $(m, n) \neq 1$, akkor mindkettő 0).

E szabályok formálisan, azonnal következnek a Legendre-szimbólum tulajdonságaiból. Csak a számolás „közbülső” lépéseiben használjuk őket.

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

$$(1) \text{ Ha } a \equiv b \pmod{m}, \text{ akkor } \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$

$$(2) \left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right) \text{ és } \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right).$$

$$(3) \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} \text{ és } \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

$$(4) \left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right) \text{ (ha } (m, n) \neq 1, \text{ akkor mindkettő } 0).$$

E szabályok formálisan, azonnal következnek a Legendre-szimbólum tulajdonságaiból. Csak a számolás „közbülső” lépéseiben használjuk őket. Például $\left(\frac{-1}{21}\right) = 1$,

A Jacobi-szimbólum tulajdonságai

Tétel (FGy4.3.2)

Tegyük fel, hogy $m, n > 1$ páratlan számok. Ekkor

- (1) Ha $a \equiv b \pmod{m}$, akkor $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.
- (2) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \left(\frac{b}{m}\right)$ és $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.
- (3) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ és $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
- (4) $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{m}{n}\right)$ (ha $(m, n) \neq 1$, akkor mindkettő 0).

E szabályok formálisan, azonnal következnek a Legendre-szimbólum tulajdonságaiból. Csak a számolás „közbülső” lépéseiben használjuk őket. Például $\left(\frac{-1}{21}\right) = 1$, de $x^2 \equiv -1 \pmod{21}$ nem oldható meg.

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia?

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377} \right)$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right)$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right)$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right)$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right)$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) =$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\begin{aligned} \left(\frac{4183}{8377}\right) &= \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \\ &= \left(\frac{-1}{3}\right) = -1, \end{aligned}$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\begin{aligned} \left(\frac{4183}{8377}\right) &= \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \\ &= \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg.} \end{aligned}$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\begin{aligned} \left(\frac{4183}{8377}\right) &= \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \\ &= \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg. Valójában } 4183 = 47 \cdot 89, \\ &\text{de ezt nem kellett észrevennünk,} \end{aligned}$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\begin{aligned} \left(\frac{4183}{8377}\right) &= \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \\ &= \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg. Valójában } 4183 = 47 \cdot 89, \\ &\text{de ezt nem kellett észrevennünk, ez a Jacobi-szimbólumok előnye.} \end{aligned}$$

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\begin{aligned} \left(\frac{4183}{8377}\right) &= \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \\ &= \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg. Valójában } 4183 = 47 \cdot 89, \end{aligned}$$

de ezt nem kellett észrevennünk, ez a Jacobi-szimbólumok előnye.

A reciprocitási tétel alkalmazásaként belátjuk a Pepin-teszt állítását.

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) =$$
$$= \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg. Valójában } 4183 = 47 \cdot 89,$$

de ezt nem kellett észrevennünk, ez a Jacobi-szimbólumok előnye. A reciprocitási tétel alkalmazásaként belátjuk a Pepin-teszt állítását.

Állítás

Ha $F_n = 2^{2^n} + 1 \geq 5$ Fermat-prím, akkor a 3 primitív gyök mod F_n .

A Jacobi-szimbólumok használata

Megoldható-e az $x^2 \equiv 4183 \pmod{8377}$ kongruencia? Itt 8377 prím.

$$\left(\frac{4183}{8377}\right) = \left(\frac{8377}{4183}\right) = \left(\frac{11}{4183}\right) = -\left(\frac{4183}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = -1, \text{ tehát nem oldható meg. Valójában } 4183 = 47 \cdot 89,$$

de ezt nem kellett észrevennünk, ez a Jacobi-szimbólumok előnye. A reciprocitási tétel alkalmazásaként belátjuk a Pepin-teszt állítását.

Állítás

Ha $F_n = 2^{2^n} + 1 \geq 5$ Fermat-prím, akkor a 3 primitív gyök mod F_n .

Pepin-teszt (FGy5.2.2)

Az $F_n = 2^{2^n} + 1 \geq 5$ pontosan akkor prím, ha $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4 -nek és $4 \equiv 1 \pmod{3}$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4 -nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$. Tehát a 3 kvadratikus nemmaradék mod F_n ,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$. Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$. Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n ,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$$o_{F_n}(3) = o_{F_n}(g^t)$$

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt $o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t). \text{ De } g \text{ rendje}$$
$$\varphi(F_n) = F_n - 1 = 2^{2^n},$$

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt $o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje

$\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így

$$o_{F_n}(3) = o_{F_n}(g),$$

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4 -nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt $o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1 , és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje

$\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így

$o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{o}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{o}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (o_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$. Ezért $\ell = 2^n$,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{gcd}(o_{F_n}(g), t))$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$. Ezért $\ell = 2^n$, vagyis $o_{F_n}(3) = 2^{2^n} = F_n - 1$.

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\text{ord}_{F_n}(g), t)$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$. Ezért $\ell = 2^n$, vagyis $o_{F_n}(3) = 2^{2^n} = F_n - 1$. Ezért van $F_n - 1$ redukált maradékosztály mod F_n ,

A Pepin-teszt bizonyítása

Tegyük föl először, hogy F_n prím. A kvadratikus reciprocitási tétel szerint $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right)$, hiszen $n \geq 1$ miatt $F_n \equiv 1 \pmod{4}$. Mivel 2^{2^n} hatványa 4-nek és $4 \equiv 1 \pmod{3}$, ezért $F_n \equiv 1 + 1 = 2 \equiv -1 \pmod{3}$.

Tehát a 3 kvadratikus nemmaradék mod F_n , és így $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ezzel a Pepin-teszt egyik irányát beláttuk.

Legyen g primitív gyök mod F_n , ekkor $t = \log_{g, F_n}(3)$ páratlan, hiszen a 3 nemmaradék. A hatvány rendjének képlete miatt

$o_{F_n}(3) = o_{F_n}(g^t) = o_{F_n}(g) / (\gcd(o_{F_n}(g), t))$. De g rendje $\varphi(F_n) = F_n - 1 = 2^{2^n}$, t pedig páratlan, ezért a nevező 1, és így $o_{F_n}(3) = o_{F_n}(g)$, azaz a 3 tényleg primitív gyök mod F_n .

Tegyük föl, hogy $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Ekkor $o_{F_n}(3)$ nem osztója $(F_n - 1)/2 = 2^{2^n-1}$ -nek. Viszont négyzetre emelve $3^{F_n-1} \equiv 1 \pmod{F_n}$, azaz $o_{F_n}(3) \mid F_n - 1 = 2^{2^n}$. Tehát $o_{F_n}(3) = 2^\ell$, ahol $\ell \leq 2^n$, de $\ell \not\leq 2^n - 1$. Ezért $\ell = 2^n$, vagyis $o_{F_n}(3) = 2^{2^n} = F_n - 1$. Ezért van $F_n - 1$ redukált maradékosztály mod F_n , így F_n prímszám. \square

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék,

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A Legendre-szimbólum tulajdonságai (FGy4.1.4).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A Legendre-szimbólum tulajdonságai (FGy4.1.4).

A kvadratikus reciprocitási tétel, $\left(\frac{2}{p}\right)$ (FGy4.2.2-3).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A Legendre-szimbólum tulajdonságai (FGy4.1.4).

A kvadratikus reciprocitási tétel, $\left(\frac{2}{p}\right)$ (FGy4.2.2-3).

A Jacobi-szimbólum tulajdonságai (FGy4.3.2).

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A Legendre-szimbólum tulajdonságai (FGy4.1.4).

A kvadratikus reciprocitási tétel, $\left(\frac{2}{p}\right)$ (FGy4.2.2-3).

A Jacobi-szimbólum tulajdonságai (FGy4.3.2).

A 3 kvadratikus maradék a Fermat-prímekre,

A 28. előadáshoz tartozó vizsgaanyag

Fogalmak

Diszkrét logaritmus (index, FGy3.4.1).

k -adik hatványmaradék, kvadratikus maradék (FGy3.5.2, 4.1.1).

Legendre-szimbólum (FGy4.1.3). Jacobi-szimbólum (FGy4.3.1).

Tételek

A binom kongruencia megoldása (FGy3.5.1).

A hatványmaradékok jellemzése, száma (FGy3.5.3).

Euler-lemma (FGy4.1.2).

A Legendre-szimbólum tulajdonságai (FGy4.1.4).

A kvadratikus reciprocitási tétel, $\left(\frac{2}{p}\right)$ (FGy4.2.2-3).

A Jacobi-szimbólum tulajdonságai (FGy4.3.2).

A 3 kvadratikus maradék a Fermat-prímekre,

Pepin-teszt (FGy5.2.2).