9.2 Legendre-symbolet

Fra før: For p odde prim og $a \in \mathbb{Z}$ med $\gcd(a,p)=1$, ønsker vi å avgjøre om

$$x^2 \equiv a \pmod p$$

er løsbar.

(1) Hvis løsbar: a kalles en <u>kvadratisk rest</u> av p

(2) Eulers kriterium: a kv. rest av $p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$

(3) Har også: a ikke kv. rest av $p \iff a^{\frac{p-1}{2}} \equiv -1 \pmod p$

(4) De $p-1$ tallene $\{1,2,\dots,p-1\}$ representerer alle tall $a \in \mathbb{Z}$ med $\gcd(a,p)=1$. Så alt koker ned til å avgjøre hvilke tall i $\{1,2,\dots,p-1\}$ som er kv. rest av p, og hvilke som ikke er det.

Eksempel: For $p=11$ er $\frac{p-1}{2}=5$, så

$$a \text{ kv. rest av } 11 \iff a^5 \equiv 1 \pmod{11}$$

For tallene $1,2,\dots,10$ har vi

$1^5 \equiv 1 \pmod{11}$
$2^5 \equiv 32 \equiv -1 \pmod{11}$
$3^5 \equiv 243 \equiv 1 \pmod{11}$
$4^5 \equiv 1024 \equiv 1 \pmod{11}$
$5^5 \equiv 3125 \equiv 1 \pmod{11}$
$6^5 \equiv (-5)^5 \equiv -5^5 \equiv -1 \pmod{11}$
$7^5 \equiv (-4)^5 \equiv -4^5 \equiv -1 \pmod{11}$
$8^5 \equiv (-3)^5 \equiv -3^5 \equiv -1 \pmod{11}$
$9^5 \equiv (-2)^5 \equiv -2^5 \equiv 1 \pmod{11}$
$10^5 \equiv (-1)^5 \equiv -1 \pmod{11}$

Så de kv. restene av 11 er $\{1,3,4,5,9\}$, og ikke-restene er $\{2,6,7,8,10\}$.

Def: La p være prim og $a \in \mathbb{Z}$ med $p \nmid a$. <u>Legendresymbolet</u> (a/p) er def ved

$$(a/p) = \begin{cases} 1 & \text{hvis } a \text{ er en kv. rest av } p \\ -1 & \text{hvis } a \text{ ikke er en kv. rest av } p \end{cases}$$

Merk: (1) Symbolet er <u>ikke</u> en brøk.

(2) Pr. def:

$(a/p)=1 \iff x^2 \equiv 1 \pmod p$ løsbar
$(a/b)=-1 \iff$ — " — ikke løsbar

Eksempel: $(1/11)=(3/11)=(4/11)=(5/11)=(9/11)=1$ mens $(2/11)=(6/11)=(7/11)=(8/11)=(10/11)=-1$

<u>Teorem 9.2</u> p odde prim, $\gcd(a,p)=\gcd(b,p)=1$.

(a) $a \equiv b \pmod p \Rightarrow (a/p)=(b/p)$
(b) $(a^2/p)=1$
(c) $(a/p) \equiv a^{\frac{p-1}{2}} \pmod p$
(d) $(ab/p)=(a/p)(b/p)$
(e) $(1/p)=1$ og $(-1/p)=(-1)^{\frac{p-1}{2}}$
(f) $(ab^2/p)=(a/p)$

Bevis: (a) $x^2 \equiv a \pmod p \Leftrightarrow x^2 \equiv b \pmod p$ siden $a \equiv b \pmod p$

(b) $x^2 \equiv a^2 \pmod p$ er løsbar.

(c) Hvis $(a/p)=1$ er $x^2 \equiv a \pmod p$ løsbar, så da er $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Det gir $a^{\frac{p-1}{2}} \equiv 1 \equiv (a/p) \pmod p$. Hvis $(a/p)=-1$ er $x^2 \equiv a \pmod p$ ikke løsbar, så da er $a^{\frac{p-1}{2}} \equiv -1 \equiv (a/p) \pmod p$.

(d) $(ab/p) \overset{(c)}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \overset{(c)}{\equiv} (a/p)(b/p) \pmod p$. Siden (ab/p), (a/p) og (b/p) er ± 1 og p er odde må da $(ab/p) = (a/p)(b/p)$.

(e) Siden $x^2 \equiv 1 \pmod p$ er løsbar er $(1/p)=1$. Fra (c) har vi $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, men $(-1/p) = \pm 1$ og $(-1)^{\frac{p-1}{2}} = \pm 1$, så vi har likhet.

(f) $(ab^2/p) \overset{(d)}{=} (a/p)(b^2/p) \overset{(b)}{=} (a/p)$. □

Eksempel: Er 170 en kv. rest av 13, dvs er $x^2 \equiv 170 \pmod{13}$ løsbar? Siden $170 = 10 \cdot 17$ har vi

$$(170/13) = (10 \cdot 17/13) = (10/13)(17/13)$$

Men $17 \equiv 4 \equiv 2^2 \pmod{13}$, så

$$(17/13) = (2^2/13) = 1$$

som gir

$$(170/13) = (10/13)(17/13) = (10/13)$$
$$\equiv 10^{\frac{13-1}{2}} \equiv 10^6 \equiv 1 \pmod{13}$$

Så 170 er en kv. rest av 13.

Teorem 9.4 Hvis p er et odde primtall er

$$\sum_{a=1}^{p-1} (a/p) = 0$$

Bevis: Fra Seksjon 8.2 vet vi at $\exists$ en primitiv rot b av p, dvs at $b^{p-1} \equiv 1 \pmod p$ og $p-1$ er minste eksponent k med $b^k \equiv 1 \pmod p$. Siden $b^{\frac{p-1}{2}}$ er kongr med enten 1 eller -1 modulo p (avhengig av om b er en kv. rest av p eller ikke), må da

$$b^{\frac{p-1}{2}} \equiv -1 \pmod p$$

For $k \geq 1$ er da

$$(b^k/p) \equiv (b^k)^{\frac{p-1}{2}} \equiv (b^{\frac{p-1}{2}})^k \equiv (-1)^k \pmod p$$

Siden $(b^k/p) = \pm 1$ og $(-1)^k = \pm 1$ må vi da ha likhet:

$$(b^k/p) = (-1)^k$$

Fra Seksjon 8.1 er de $p-1$ tallene

$$b, b^2, \ldots, b^{p-1}$$

inkongr. modulo p, så de må være kongr med

$$1, 2, \ldots, p-1$$

i en eller annen rekkefølge. Legendre-symbolet er invariant under kongruens, så

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{k=1}^{p-1} \left(\frac{b^k}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0 \qquad \square$$

Konsekvens: Halvparten av tallene i mengden $\{1, 2, \ldots, p-1\}$ er kv. rester av p, den andre halvparten ikke.

Eksempel: For $p = 11$ så vi at $\{1, 3, 4, 5, 9\}$ er kv. rester, mens $\{2, 6, 7, 8, 10\}$ ikke er det:

$$\sum_{a=1}^{11-1} \left(\frac{a}{11}\right) = \left(\frac{1}{11}\right) + \left(\frac{2}{11}\right) + \cdots + \left(\frac{10}{11}\right)$$

$$= 1 - 1 + 1 + 1 + 1 - 1 - 1 - 1 + 1 - 1$$

$$= 0$$