8.2 Primitive røtter for primtall

Har sett: For $\gcd(a,n)=1$ gir ET at $a^{\phi(n)} \equiv 1 \pmod n$

(1) Ordenen til a modulo n er minste $k>1$ med $a^k \equiv 1 \pmod n$ (så $k \le \phi(n)$)

(2) Hvis ordenen er $\phi(n)$ er a en primitiv rot av n.

(3) Hvis ordenen er k: (i) $a^t \equiv 1 \pmod n \iff k \mid t$

(ii) a^t har orden $k/\gcd(k,t)$ modulo n

(iii) $a, a^2, \dots, a^k$ er inkongr modulo n

(4) Hvis n har en primitiv rot, så har den $\phi(\phi(n))$ stykker.

Eksempler: (1) For $n=8$ er $\phi(n)=4$. Tallene 1,3,5,7 representerer alle $a \in \mathbb{Z}$ med $\gcd(a,8)=1$.

Siden $1^1 \equiv 1 \pmod 8$

$3^2 \equiv 1 \pmod 8$

$5^2 \equiv 1 \pmod 8$

$7^2 \equiv 1 \pmod 8$

har 8 ingen pr. røtter: det finnes ingen $a \in \mathbb{Z}$ med orden $\phi(8)$ modulo 8

(2) Se på $n=18$. Har $\phi(18) = \phi(2 \cdot 3^2) = 2 \cdot 3^2 (1-1/2)(1-1/3) = 6$. De 6 tallene i mengden $\{1,2,\dots,18\}$ rel. pr. med 18 er disse:

$$1, 5, 7, 11, 13, 17$$

Har 18 noen pr. røtter? Siden $\phi(18)=6$ må ordenen til et tall være 1, 2, 3 eller 6.

$1^1 \equiv 1 \pmod{18}$

$5^1 \equiv 1,\ 5^2 \equiv 7,\ 5^3 \equiv 17 \pmod{18}$, så 5 er pr. rot

$7^1 \equiv 7,\ 7^2 \equiv 13,\ 7^3 \equiv 1 \pmod{18}$

$11^1 \equiv 11,\ 11^2 \equiv 13,\ 11^3 \equiv 17 \pmod{18}$, så 11 er pr. rot

$13^1 \equiv 13,\ 13^2 \equiv 7,\ 13^3 \equiv 1 \pmod{18}$

$17^1 \equiv 17,\ 17^2 \equiv 1 \pmod{18}$

Så 18 har to pr. røtter: 5 og 11. Merk: $\phi(\phi(18)) = \phi(6) = 2$.

Skal vise: p prim $\Rightarrow$ p har en pr. rot ($\exists\, a \in \mathbb{Z}$ med orden $\phi(p)=p-1$ modulo p)

Teorem 8.5 (Lagrange)

La p være et primtall og

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

et polynom med $a_i \in \mathbb{Z}$ og $p \nmid a_n$. Da har kongr

$$f(x) \equiv 0 \pmod p$$

maksimalt n inkongr. løsn modulo p.

Bevis: Induksjon på n. For $n=1$ er $f(x)=a_1x+a_0$, så da blir kongruensen

$$a_1x \equiv -a_0 \pmod p$$

Siden $\gcd(p,a_1)=1$ vet vi da at denne har nøyaktig én løsn modulo p. La nå $n>1$, og anta utsagnet stemmer for alle polynomer av grad $n-1$. Hvis $f(x)\equiv 0 \pmod p$ ikke har løsn, så er vi ferdige. Anta derfor en løsn finnes: $\exists\, a\in\mathbb{Z}$ med $f(a)\equiv 0 \pmod p$. Div alg for polynomer gir

$$f(x)= q(x)(x-a)+r$$

hvor $r\in\mathbb{Z}$. Polynomet $q(x)$ har da grad $n-1$. Siden

$$0\equiv f(a)\equiv q(a)(a-a)+r \equiv r \pmod p$$

er $f(x)\equiv q(x)(x-a) \pmod p$, dvs denne kongr. gjelder $\forall x$. Anta nå at b er en løsn av $f(x)\equiv 0 \pmod p$, og at $b\not\equiv a \pmod p$. Da er $p\nmid(b-a)$, så $\gcd(p,b-a)=1$. Vi har

$$0\equiv f(b)\equiv q(b)(b-a) \pmod p$$

og kan dele ut $b-a$ og få

$$0\equiv q(b) \pmod p$$

Ved induksjon har $q(x)\equiv 0 \pmod p$ maks $n-1$ løsn, så $f(x)\equiv 0 \pmod p$ har maks n løsn. □

Korollar: Hvis p er et primtall og $d\mid(p-1)$, så har

$$x^d-1 \equiv 0 \pmod p$$

nøyaktig d løsn.

Bevis: Bruker Lagranges teorem.

Teorem 8.6 Hvis p er et primtall og $d\mid(p-1)$, så finnes det $\phi(d)$ inkongruente tall som har orden d modulo p.

Bevis: Se på tallene $\{1,2,\dots,p-1\}$. Vi vet at ordenen til et tall deler $\phi(p)=p-1$, så hvis vi lar

$$\psi(d)= \text{antall } a\in\{1,2,\dots,p-1\} \text{ med orden } d \text{ modulo } p$$

så er $\sum_{d\mid(p-1)} \psi(d) = p-1$. Fra Teorem 7.5 har vi også $\sum_{d\mid(p-1)} \phi(d) = p-1$, så vi får

$$\sum_{d\mid(p-1)} \psi(d) = \sum_{d\mid(p-1)} \phi(d)$$

Siden $\psi(d)\geq 0$ og $\phi(d)\geq 0$ vil vi da ha at $\psi(d)=\phi(d)$ for alle $d\mid(p-1)$ hvis vi klarer å vise at $\psi(d)\leq\phi(d)$.

La $d \mid (p-1)$. Hvis $\psi(d) \neq 0$ finnes en $a \in \mathbb{Z}$ med orden d modulo p.

Har sett at da er

$$a, a^2, \dots, a^d$$

inkongruente modulo p. Siden $(a^i)^d \equiv (a^d)^i \equiv 1^i \equiv 1 \pmod{p}$ er alle disse d tallene en løsn av

$$x^d \equiv 1 \pmod{p}.$$

Fra Lagranges teorem er det ikke flere løsn av denne, så tallene

$$a, a^2, \dots, a^d$$

inneholder alle tallene som har orden d modulo p. Vi vet også at siden a har orden d, så har a^t orden $d/\gcd(t,d)$ modulo p. Dette blir d hvis og bare hvis $\gcd(t,d)=1$, så

$$\begin{aligned}\psi(d) &= \text{antall inkongr. tall av orden } d \text{ modulo } p \\ &= \text{antall elementer i } \{a, a^2, \dots, a^d\} \text{ av orden } d \text{ modulo } p \\ &= \text{antall } t \in \{1,2,\dots,d\} \text{ med } \gcd(t,d)=1 \\ &= \phi(d)\end{aligned}$$

□

Korollar: p prim $\Rightarrow p$ har $\phi(p-1)$ primitive røtter.

Kan vises: Et tall n har pr. røtter hvis og bare hvis n er på én av følgende former

$$1, 2, 4, p^t, 2p^t$$

hvor p er et odde primtall og $t \geq 1$.