

# Talteori, Föreläsning 5

## Primitiva rötter

Jan Snellman<sup>1</sup>

<sup>1</sup>Matematiska Institutionen

Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan <http://courses.mai.liu.se/GU/TATA54/>



**TEKNISKA HÖGSKOLAN**  
LINKÖPING UNIVERSITET

## Multiplikativ ordning

Definition

Elementära egenskaper

## Primitiva rötter

Definition

Primitiva rötter modulo ett primtal

Primitiva rötter modulo en  
primkvadrat

Primitiva rötter modulo en primpotens

Tvåpotenser

Generellt modulus

## Universell exponent

Struktur av  $\mathbb{Z}_n^*$

## Indexaritmetik

Indexregler

Lösa kongruenser

Potensresidyer

## Definition

- ▶  $G$  ändlig grupp,  $g \in G$ .
- ▶  $g^i * g^j = g^{i+j}$ .
- ▶  $g \in G$  har ordning  $o(g) = n$  om  $g^n = 1$  men  $g^m \neq 1$  för  $1 \leq m < n$ ;  $o(e) = 1$
- ▶  $g^s = 1$  omm  $n|s$ .
- ▶  $g^i = g^j$  omm  $i \equiv j \pmod n$ .
- ▶  $a \in \mathbb{Z}$  har (multiplikativ) ordning  $n$  modulo  $m$  om  $o([a]_m) = n$ , i.e. om  $a^n \equiv 1 \pmod m$  men ej för mindre potens.
- ▶ Rosens notation:  $\text{ord}_m(a) = n$

$$\text{ord}_7(3) = 6$$

$$G = \mathbb{Z}_n^\times = \{ [k]_n : \gcd(k, n) = 1 \}$$

$$o([3]_7) = 6, [1]_7 \in \mathbb{Z}_7^\times$$

## Teorem

$g \in G$  grupp,  $o(g) = n$ . Då  $o(g^k) = \frac{n}{\gcd(n,k)}$

$$\left\{ \begin{array}{l} o(g) = 4, \quad 1^4 = 1 \\ o(g^2) = 2, \quad (g^2)^2 = 1 \end{array} \right.$$

## Bevis.

Sätt  $d = \gcd(n, k)$ . Har  $(g^k)^s = g^{ks} = 1$  omm  $n | ks$ , alltså omm  $(n/d) | (k/d)s$ . Men  $\gcd((n/d), (k/d)) = 1$ , så detta inträffar omm  $(n/d) | s$ . Alltså  $o(g^k) = (n/d)$ .  $\square$

## Exempel

I  $\mathbb{Z}_{13}^*$ ,  $o([4]) = 6$ , ty  $[4]^2 = [3], [4]^3 = [12], [4]^4 = [9], [4]^5 = [10], [4]^6 = [1]$ . Så

$$e = [1]_{13}$$

$$o([4]^4) = 4 / \gcd(4, 6) = 6/2 = 3.$$

$$|\mathbb{Z}_{13}^*| = 12$$

Vi ser att  $[4]^4 = [9], [4]^8 = [13], [4]^{12} = [1]$

$$G = \langle \cdot \rangle^*$$

## Teorem

$g, h \in G$  grupp,  $gh = hg$ ,  $o(g) = m$ ,  $o(h) = n$ ,  $\gcd(m, n) = 1$ . Då  $o(gh) = mn$ .

## Bevis

Sätt  $o(gh) = r$ .

$$(gh)^{mn} = (gh)(gh) \cdots (gh) = g^{mn} h^{mn} = (g^m)^n * (h^n)^m = 1^n * 1^m = 1,$$

så  $r | mn$ .

Eftersom  $\gcd(m, n) = 1$  så är  $r = r_1 r_2$  med  $r_1 | m$ ,  $r_2 | n$ ,  $\gcd(r_1, r_2) = 1$ .

Så

$$1 = (gh)^r = (gh)^{r_1 r_2} = g^{r_1 r_2} h^{r_1 r_2}.$$

### Bevis.

Då gäller alltså att

$$1 = 1^{s_1} = g^{r_1 s_1 r_2} h^{r_1 s_1 r_2} = (g^m)^{r_2} h^{mr_2} = h^{mr_2}.$$

Det följer att  $n \mid (mr_2)$ . Men  $\gcd(n, m) = 1$ , så  $n \mid r_2$ . Alltså  $r_2 = n$ .

På liknande sätt får vi att  $r_1 = m$ .

Följaktligen så är  $r = mn$ .



## Exempel

Om  $g = h = [4] \in \mathbb{Z}_{13}^*$ , så  $o(g) = 6$ ,  $o(gh) = o(g^2) = 6/2 = 3$  enligt tidigare. Så det gäller INTE NÖDVÄNDIGTVIS att

$$o(gh) = \text{lcm}(o(g), o(h))$$

när  $\gcd(o(g), o(h)) > 1$ .

## Definition

Heltalet  $a$  är en *primitiv rot* modulo  $n$  om  $[a]_n$  genererar  $\mathbb{Z}_n^*$ , i.e., om den har multiplikativ ordning  $\phi(n)$ .

$$\# \{ 1 \leq k \leq n-1 : \gcd(k, n) = 1 \}$$

## Exempel

- 2 är en primitiv rot modulo 5, enär

$$\varphi(5) = 5 - 1 = 4$$

$$[2]_5^1 = [2], [2]_5^2 = [4], [2]_5^3 = [3], [2]_5^4 = [1]_5$$

- Det finns inga primitiva rötter modulo 8, eftersom  $\mathbb{Z}_8^*$  har  $\phi(8) = 4$  element, men inget element har ordning  $> 2$ :

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$\mathbb{Z}_5^*$$

$$g^2 = 1 \text{ alla } g \in \mathbb{Z}_8^*$$

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1



## Teorem

$p$  primtal,  $d$  delar  $p - 1$ . Då har polynomet  $f(x) = x^d - 1 \in \mathbb{Z}_p[x]$  exakt  $d$  nollställen.

## Bevis.

- ▶  $e = (p - 1)/d$   $ed = p - 1$
- ▶  $x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1)(x^{de-d} + x^{de-2d} + \dots + x^d + 1) = (x^d - 1)g(x)$   $\uparrow \quad g(x)$   $\downarrow \quad \downarrow$
- ▶  $\deg(g(x)) = de - d = p - 1 - d$
- ▶ Fermat:  $x^{p-1} - 1$  har  $p - 1$  nollställen
- ▶ Lagrange:  $x^d - 1$  har högst  $d$  nollställen,  $g(x)$  högst  $p - 1 - d$  nollställen
- ▶ Slutsats:  $x^d - 1$  har precis  $d$  nollställen, ( $g(x)$  har precis  $p - 1 - d$  nollställen)



## Teorem

$p$  primtal. Då finns en primitiv rot modulo  $p$ .

$$g^{12} = 1 \text{ men } g^6 \neq 1$$

## Bevis.

- ▶ Ok när  ~~$p = 2$~~
- ▶ Antag  $p$  udda
- ▶ Faktorisera  $p - 1 = q_1^{a_1} \cdots q_r^{a_r}$
- ▶  $h_1(x) = x^{q_1^{a_1}} - 1$  har precis  $q_1^{a_1}$  nollställen enligt föregående
- ▶  $\hat{h}_1(x) = x^{q_1^{a_1-1}} - 1$  har precis  $q_1^{a_1-1}$  nollställen
- ▶ Exakt  $q_1^{a_1} - q_1^{a_1-1}$  element  $v \in \mathbb{Z}_p^*$  med  $v^{q_1^{a_1}} = 1$ ,  $v^{q_1^{a_1-1}} \neq 1$
- ▶ Dessa är precis de som har ordning  $q_1^{a_1}$ , välj en,  $u_1$
- ▶  $u = u_1 u_2 \cdots u_r$
- ▶  $o(u) = o(u_1) \cdots o(u_r) = q_1^{a_1} \cdots q_r^{a_r} = p - 1$ , ty  $u_i$  parvis relativt prima

$$\begin{aligned} d &= q_1^{a_1} \mid (p-1) \\ \hat{d} &= q_1^{a_1-1} \mid (p-1) \end{aligned}$$

Giltig lemmat



## Exempel

```
p=nth_prime(362)
print(p)
myfact=factor(p-1)
print(myfact)
c=mod(1,p)
C=Set([])
```

```
for fact in myfact:
```

```
    q,a=fact
```

```
    b=a-1
```

```
    h=Integers(p)[x](x^(q^a)-1)
```

```
    hh=Integers(p)[x](x^(q^b)-1)
```

```
maxl = Set(h.roots(multiplicities=False))
minl = Set(hh.roots(multiplicities=False))
candidates = maxl.difference(minl)
u = candidates[0]
print(hh,h,maxl,minl,u)
c = c*u
C=C.union(Set([u]))
print(C,c)
print(multiplicative_order(c))
```

ger  $p = 2441$ ,  $p - 1 = 2440 = 2^3 \cdot 5 \cdot 61$ ,  $C = \{1280, 1122, 590\}$ ,  $c = 2275$ ,  $\text{ord}_p(c) = 2440$ .

primitive root mod 2441  
order: 2440

## Teorem

$p$  primtal. Då finns en primitiv rot modulo  $p^2$ .

$$p > 2$$

## Bevis

1.  $a$  primitiv rot mod  $p$
2.  $g = a + tp$  *lyft!*
3.  $h = \text{ord}_{p^2}(g)$
4.  $\phi(p^2) = p(p-1)$ , så  $h | p(p-1)$
5.  $g^h \equiv 1 \pmod{p^2}$  och alltså  $g^h \equiv 1 \pmod{p}$
6.  $g \equiv a \pmod{p}$  så  $g^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$
7. Vi får  $(p-1) | h$
8. Så  $h = p(p-1)$  eller  $h = p-1$
9. Hävdar: båda fallen kan inträffa (beroende på  $t$ ). Speciellt, kan välja  $t$  så att  $h = p(p-1)$ , och  $g$  primitiv rot mod  $p^2$

$$\# \mathbb{Z}_{p^2}^* = p^2 - p$$

*?*

## Bevis.

10. Sätt  $f(x) = x^{p-1} - 1$
11.  $f(a) \equiv 0 \pmod p$ . Vill undersöka om  $g = a + tp$  är ett lyft.
12.  $f'(x) = (p-1)x^{p-2} \equiv -x^{p-2} \pmod p$
13.  $f'(a) \equiv -a^{p-2} \pmod p \not\equiv 0 \pmod p$
14. Så unikt  $t = t_0$  för vilket  $g = a + t_0p$  lyft
15. För andra  $t$ ,  $g = a + tp$  ej lyft,  $f(g) \not\equiv 0 \pmod{p^2}$ ,  $g^{p-1} \not\equiv 1 \pmod{p^2}$
16. Dvs,  $\text{ord}_{p^2}(g) \neq p-1$ .
17. Enligt tidigare,  $\text{ord}_{p^2}(g) = p(p-1)$
18.  $g = a + tp$  primitiv rot modulo  $p^2$  för alla  $t$  utom ett!



## Exempel

- ▶ Fungerar för  $p = 2$  (degenererat fall)
- ▶  $\mathbb{Z}_2^* = \{[1]_2\}$ . Primitiv rot 1
- ▶ Lyfter till 1, 3
- ▶ 3 är en primitiv rot mod 4.

## Exempel

Kontrollerar att 2 är en primitiv rot modulo 11. Sen försöker vi lyfta:

```
p,a=11,2
thelifts = [
    [a+t*p,multiplicative_order(mod(a+t*p,p^2))]
    for t in range(p)]
```

ger

$[[2, 110], [13, 110], [24, 110], [35, 110]]$

$[[57, 110], [68, 110], [79, 110], [90, 110], [101, 110], [112, 10]]$

Så varje lyft är en primitiv rot mod  $11^2$ , *utom*  $2 + 10 * 11$ .

## Teorem

1.  $p > 2$  primtal
2.  $a$  primitiv rot modulo  $p^k$
3.  $k \geq 2$

Då är **varje** lyft  $g = a + tp^k$  en primitiv rot modulo  $p^{k+1}$ .

## Bevis.

Konsultera "Constructing the Primitive Roots of Prime Powers" av Nathan Jolly (finns på kurshemsidan). □



## Exempel

- ▶  $p = 11, k = 2$
- ▶  $a = 2$  primitiv rot mod  $p$  och mod  $p^2$
- ▶ Alla dess lyft skall vara primitiva rötter mod  $p^3$
- ▶ Speciellt,  $a$  själv
- ▶ Kontroll:  $\phi(p^3) = p^2(p - 1) = 1210$
- ▶ Faktiskt,  $\text{ord}_{11^3}(2) = 1210$ .

## Teorem

- ▶ 1 primitiv rot mod 2
- ▶ 3 primitiv rot mod 4
- ▶ Ingen primitiv rot mod 8
- ▶ Inte för något  $2^k$ ,  $k \geq 3$
- ▶ I själva verket, om  $k \geq 3$ ,  $a$  udda (så  $\gcd(a, 2^k) = 1$ ) har vi

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

## Bevis.

Läs Rosen!



## Teorem

- ▶  $p$  udda primtal
- ▶  $k \in \mathbb{Z}_+$
- ▶ Varje primitiv rot mod  $p^k$  lyfter till  $2p^k$
- ▶ Så  $n = 2p^k$  har primitiva rötter
- ▶ Primitiv rot modulo  $m$  om  $m$  är 2, 4,  $p^k$  eller  $2p^k$

3.5

## Bevis.

Rosen!



## Definition

- ▶  $n \in \mathbb{Z}_+$
- ▶  $U$  är en **universell exponent** till  $n$  om  $[a]_n^U = [1]_n$  för alla  $[a] \in \mathbb{Z}_n^*$
- ▶ Id est, om  $a^U \equiv 1 \pmod n$  för alla  $a$  med  $\gcd(a, n) = 1$ .
- ▶  $\lambda(n)$  är den **minsta universella exponenten**

## Exempel

Ordning av elem. i  $\mathbb{Z}_9^*$ :

$g$	1	2	4	5	7	8
$o(g)$	1	6	3	6	3	2

$$\lambda(9) = 6.$$

## Exempel

- ▶  $\mathbb{Z}_5^* \simeq C_4$
- ▶  $\mathbb{Z}_8^* \not\simeq \mathbb{Z}_5^*$ , ty ej cyklisk, båda har 4 element

## Teorem (Struktur av $Z_n^*$ )

- ▶  $\mathbb{Z}_2^*$  trivial,  $\mathbb{Z}_4^* \simeq C_2$ ,  $\mathbb{Z}_8^* \simeq C_2 \times C_2$ , och  $\mathbb{Z}_{2^k}^* \simeq C_2 \times C_{2^{k-2}}$
- ▶  $p$  udda primtal
- ▶  $\mathbb{Z}_{p^a}^* \simeq C_s$  med  $s = \phi(p^a)$
- ▶ Om  $n = p_1^{a_1} \cdots p_r^{a_r}$  så  $\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{a_r}}^*$
- ▶  $\lambda(2) = 1$ ,  $\lambda(4) = 2$ ,  $\lambda(2^k) = 2^{k-2}$ ,  $\lambda(p^a) = \phi(p^a) = p^a - p^{a-1}$
- ▶  $\lambda(p_1^{a_1} \cdots p_r^{a_r}) = \text{lcm}(\lambda(p_1^{a_1}), \dots, \lambda(p_r^{a_r}))$

## Bevis för sista delen.

Om  $G = C_{m_1} \times C_{m_2} \times C_{m_r}$ , med  $m = \text{lcm}(m_1, \dots, m_r)$ , så

- ▶  $h^m = 1$  för alla  $h \in G$
- ▶ Finns något  $g \in G$  med  $o(g) = m$



## Exempel

- ▶  $675 = 27 * 25$
- ▶  $\phi(27) = 18, \phi(25) = 20$
- ▶  $\phi(675) = \phi(27)\phi(25) = 18 * 20 = 360$
- ▶  $\lambda(675) = \text{lcm}(18, 20) = 180$
- ▶  $\mathbb{Z}_{675}^* \simeq C_{18} \times C_{20}$

- ▶  $m = p^k$  eller  $m = 2p^k$
- ▶  $\phi(m) = M$
- ▶  $\mathbb{Z}_m^* = \langle r \rangle = \{r, r^2, \dots, r^M = [1]_m\} \simeq C_M$
- ▶  $[a]_m \in \mathbb{Z}_m^*$ , i.e.  $\gcd(a, m) = 1$
- ▶  $a \equiv r^x \pmod{m}$  för unikt  $x$  med  $1 \leq x \leq M$
- ▶  $x = \text{ind}_r(a)$ , index av  $a$  till basen  $r$ , diskret logaritm
- ▶  $a, b$  relativt prima med  $m$ , då  $\text{ind}_r(a) = \text{ind}_r(b)$  om och endast om  $a \equiv b \pmod{m}$  i.e. om  $[a]_m = [b]_m$



## Exempel

- ▶  $n = 14$
- ▶  $\phi(n) = 6$
- ▶  $r = 3$
- ▶  $\text{ord}_{14}(r) = 6$
- ▶  $[r, r^2, r^3, r^4, r^5, r^6] = [3, 9, 13, 11, 5, 1]$
- ▶  $\text{ind}_{14}(13) = 3$ , etc

### Teorem

$$\phi(m) = M, \mathbb{Z}_m^* = \langle r \rangle.$$

- ▶  $\text{ind}_r(1) \equiv 0 \pmod{M}$
- ▶  $\text{ind}_r(ab) \equiv \text{ind}_r(a) + \text{ind}_r(b) \pmod{M}$
- ▶  $k \in \mathbb{Z}_+$
- ▶  $\text{ind}_r(a^k) \equiv k * \text{ind}_r(a) \pmod{M}$

Precis som vanliga logaritmer!

## Exempel

$$9^x \equiv 11 \pmod{14}$$

$$\text{ind}_3(9^x) = \text{ind}_3(11)$$

$$x * \text{ind}_3(9) \equiv \text{ind}_3(11) \pmod{6}$$

$$x * 2 \equiv 4 \pmod{6}$$

$$x \equiv 2 \pmod{3}$$

Kontroll:  $9^2 = 81 = 5 * 14 + 11 \equiv 11 \pmod{14}$ ,

$9^5 \equiv 9(9^2)^2 \equiv 9 * 11^2 \equiv 9 * (-3)^2 \equiv 9 * 9 \equiv 11 \pmod{14}$ .

## Definition

- ▶  $m, k \in \mathbb{Z}_+$
- ▶  $a \in \mathbb{Z}, \gcd(a, m) = 1$
- ▶  $x^k \equiv a \pmod{m}$  lösbar
- ▶ Då:  $a$  är en  $k$ :e potens-residy av  $m$

## Exempel

- ▶  $m = 11, k = 2$
- ▶  $x^4 \equiv 9 \pmod{11}$  lösbar, så 9 är fjärdepotens-residy mod 11
- ▶  $x^4 \equiv 8 \pmod{11}$  ej lösbar, så 8 ej fjärdepotens-residy mod 11
- ▶  $x^4 \pmod{11}$  är  $[0, 1, 5, 4, 3, 9, 9, 3, 4, 5, 1]$

## Teorem

►  $m \in \mathbb{Z}_+, M = \phi(m), \mathbb{Z}_m^* = \langle [r]_m \rangle$

►  $k \in \mathbb{Z}_+, a \in \mathbb{Z}, \gcd(a, m) = 1$

►  $d = \gcd(k, M)$

► Då:

$$x^k \equiv a \pmod{m}$$

*lösbar om*

$$a^{M/d} \equiv 1 \pmod{m}$$

► Om lösbar, precis  $d$  lösningar mod  $m$  (dvs i  $\mathbb{Z}_m^*$ )

## Bevis.

Översätt till

$$k * \text{ind}_r(x) \equiv \text{ind}_r(a) \pmod{M}$$

Skriv  $x \equiv r^y \pmod{m}$ ,  $\text{ind}_r(a) = A$ .

Får

$$k * y \equiv A \pmod{M}$$

Lösbart omm  $d|A$ . Men

$$A = dz \iff \frac{M}{d}A = Mz$$

så det sker omm  $\frac{M}{d}A \equiv 0 \pmod{M}$ , alltså omm

$$a^{\frac{M}{d}} \equiv 1 \pmod{m}$$



## Exempel

►  $m = 11, M = 10, k = 4, d = 2$



$$9^5 \equiv 1 \pmod{11}$$

►  $x^4 \equiv 9 \pmod{11}$  lösbar



$$8^5 \equiv -1 \pmod{11}$$

►  $x^4 \equiv 8 \pmod{11}$  ej lösbar