Number Theory, Lecture 5

Primitive roots

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Summary

Summary

Definition

- G finite group, $g \in G$.
- $g^i * g^j = g^{i+j}$.
- $g \in G$ has order $o(g) = n$ if $g^n = 1$ but $g^m \neq 1$ for $1 \leq m < n$; $o(e) = 1$
- $g^s = 1$ iff $n|s$.
- $g^i = g^j$ iff $i \equiv j \mod n$.
- a has (multiplicative) order n modulo m if $o([a]_m) = n$, i.e. if $a^n \equiv 1 \mod m$ but not for smaller power.
- (New) $\mathrm{ord}_m(a) = n$

Theorem

$g \in G$ *group,* $o(g) = n$. *Then* $o(g^k) = \frac{n}{\gcd(n,k)}$

Proof.

Put $d = \gcd(n,k)$. Have $(g^k)^s = g^{ks} = 1$ iff $n|ks$, thus iff $(n/d)|(k/d)s$. But $\gcd((n/d),(k/d)) = 1$, so occurs iff $(n/d)|s$. Hence $o(g^k) = (n/d)$. □

Example

In $\mathbb{Z}_{13}^*$, $o([4]) = 6$, since $[4]^2 = [3], [4]^3 = [12], [4]^4 = [9], [4]^5 = [10], [4]^6 = [1]$. Hence $o([4]^4) = 4/\gcd(4,6) = 6/2 = 3$. Indeed $[4]^4 = [9]$, $[4]^8 = [13]$, $[4]^{12} = [1]$

Picture of 12-hour clock

Theorem

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

Proof

Put $o(gh) = r$.

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

so $r|mn$. Since $\gcd(m, n) = 1$, $r = r_1 r_2$ with $r_1 s_1 = m$, $r_2 s_2 = n$, $\gcd(r_1, r_2) = 1$. So

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

Then

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

Proof.

Hence $n|(mr_2)$. But $\gcd(n,m)=1$, so $n|r_2$. Hence $r_2=n$.
Similarly, $r_1=m$, and $r=mn$. □

Example

If $g = h = [4] \in \mathbb{Z}_{13}^*$, then $o(g) = 6$, $o(gh) = o(g^2) = 6/2 = 3$ by the earlier result. So it is not the case that

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

when $\gcd(o(g), o(h)) > 1$.

Definition

The integer a is a *primitive root* modulo n if $[a]_n$ generates $\mathbb{Z}_n^*$, i.e., if it has multiplicative order $\phi(n)$.

Example

- 2 is a primitive root modulo 5, since

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

- There are not primitive roots modulo 8, since $\mathbb{Z}_8^*$ has $\phi(8) = 4$ elements, but no element has order > 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

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

Theorem

p prime, d divides $p-1$. Then the polynomial $f(x) = x^d - 1 \in \mathbb{Z}_p[x]$ has exactly d roots.

Proof.

- $e = (p-1)/d$
- $x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1)(x^{de-d} + x^{de-2d} + \cdots + x^d + 1) = (x^d - 1)g(x)$
- $\deg(g(x)) = de - d = p - 1 - d$
- Fermat: $f(x)$ has $p-1$ roots
- Lagrange: $x^d - 1$ at most d roots, $g(x)$ at most $p-1-d$ roots
- Conclude: $x^d - 1$ has precisely d roots, ($g(x)$ has precisely $p-1-d$ roots)

□

Theorem

p prime. Then there exists a primitive root modulo p.

Proof.

- Ok when $p = 2$
- Assume p odd
- Factor $p-1 = q_1^{a_1} \cdots q_r^{a_r}$
- $h_1(x) = x^{q_1^{a_1}} - 1$ has exactly $q_1^{a_1}$ roots
- $\widehat{h}_1(x) = x^{q_1^{a_1-1}} - 1$ has exactly $q_1^{a_1-1}$ roots
- Exactly $q_1^{a_1} - q_1^{a_1-1}$ elems $v \in \mathbb{Z}_p^*$ with $v^{q_1^{a_1}} = 1$, $v^{q_1^{a_1-1}} \neq 1$
- These fellows have order $q_1^{a_1}$, pick one, u_1
- $u = u_1 u_2 \cdots u_r$
- $o(u) = o(u_1) \cdots o(u_r) = q_1^{a_1} \cdots q_r^{a_r} = p-1$.

□

Example

```
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)
```

gives $p = 2441$, $p - 1 = 2440 = 2^3 \cdot 5 \cdot 61$, $C = \{1280, 1122, 1478\}$, $c = 2141$, $\mathrm{ord}_p(c) = 2440$.

Theorem

p prime. Then there exists a primitive root modulo p^2.

Proof

1. a primitive root mod p
2. $g = a + tp$
3. $h = \mathrm{ord}_{p^2}(g)$
4. $\phi(p^2) = p(p-1)$, so $h | p(p-1)$
5. $g^h \equiv 1 \mod p^2$ and thus $g^h \equiv 1 \mod p$
6. $g \equiv a \mod p$ hence $g^{p-1} \equiv a^{p-1} \equiv 1 \mod p$
7. Thus $(p-1)|h$
8. So $h = p(p-1)$ or $h = p-1$
9. Claim: both cases occur (depending on t). In particular, can choose t such that $h = p(p-1)$, and g primitive root mod p^2

Proof.

(i) Put $f(x) = x^{p-1} - 1$

(ii) $f(a) \equiv 0 \mod p$. Want to see if $g = a + tp$ is a lift.

(iii) $f'(x) = (p-1)x^{p-2} \equiv -x^{p-2} \mod p$

(iv) $f'(a) \equiv -a^{p-2} \mod p \not\equiv 0 \mod p$

(v) So unique $t = t_0$ for which $g = a + t_0 p$ lifts

(vi) For other t, $g = a + tp$ does not lift, $f(g) \not\equiv 0 \mod p$, $g^{p-1} \not\equiv 1 \mod p^2$

(vii) By earlier, $\mathrm{ord}_{p^2}(g) = p(p-1)$

(viii) $g = a + tp$ primitive root modulo p^2 for all t but one!

□

Example

- This works for $p = 2$
- $\mathbb{Z}_2^* = \{[1]_2\}$. Primitive root 1
- Lifts to $1, 3$
- 3 is a primitive roots mod 4.

Example

We check that 2 is a primitive root modulo 11. Then, we try to lift:

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

gives

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

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

So every lift of the primitive root mod 11 is a primitive root mod 11^2, *except* $2 + 10 * 11$.

Theorem

1. $p > 2$ *a prime*
2. *a primitive root modulo* p^k
3. $k \geq 2$

Then any lift $g = a + tp^k$ *is a primitive root modulo* p^{k+1}.

Proof.

Check the article "Constructing the Primitive Roots of Prime Powers" by Nathan Jolly (on homepage). □

Example

- $p = 11$, $k = 2$
- $a = 2$ primitive root mod p and mod p^2
- All its lift should be primitive roots mod p^3
- In particular, a itself
- Check: $\phi(p^3) = p^2(p-1) = 1210$
- Indeed, $\mathrm{ord}_{11^3}(2) = 1210$.

Theorem

- *1 primitive root mod 2*
- *3 primitive root mod 4*
- *No primitive root mod 8*
- *Not for any* 2^k, $k \geq 3$
- *In fact, if* $k \geq 3$, *a odd (so* $\gcd(a, 2^k) = 1$*) then*

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

Proof.

Read all about it in Rosen! □

Theorem

- *p odd prime*
- $k \in \mathbb{P}$
- *Any primitive root mod* p^k *lifts to* $2p^k$
- *Thus,* $n = 2p^k$ *has primitive roots*
- *Primitive root modulo m iff m is 2, 4,* p^k *or* $2p^2$

Proof.

Rosen! □

Definition

- $n \in \mathbb{P}$
- U is an universal exponent of n if $[a]_n^U = [1]_n$ for all $[a] \in \mathbb{Z}_n^*$
- Id est, if $a^U \equiv 1 \mod n$ for all a with $\gcd(a,n) = 1$.
- $\lambda(n)$ is the smallest universal exponent

Example

Orders of elems in $\mathbb{Z}_9^*$:

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

The smallest universal exponent is 6.

Example

- $(\mathbb{Z}_5^*, *) \simeq (\mathbb{Z}_4, +)$, since both cyclic, 4 elems
- $\mathbb{Z}_8^* \not\simeq \mathbb{Z}_5^*$, both 4 elems, first not cyclic

Theorem (Structure of Z_n^*)

- $\mathbb{Z}_2^*$ *trivial*, $\mathbb{Z}_4^* \simeq C_2$, $\mathbb{Z}_8^* \simeq C_2 \times C_2$, *and* $Z_{2^k}^* \simeq C_2 \times C_{2^{k-2}}$
- p *odd prime*
- $\mathbb{Z}_{p^a}^* \simeq C_s$ *with* $s = \phi(p^a)$
- *If* $n = p_1^{a_1} \cdots p_r^{a_r}$ *then* $Z_n^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{a_r}}^*$
- $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^k) = 2^{k-2}$, $\lambda(p^a) = \phi(p^a) = p^a - p^{a-1}$
- $\lambda(p_1^{a_1} \cdots p_r^{a_r}) = lcm(\lambda(p_1^{a_1}), \ldots, \lambda(p_r^{a_r}))$

Proof of the last part.

If $G = C_{m_1} \times C_{m_2} \times C_{m_r}$, with $m = \operatorname{lcm}(m_1, \ldots, m_r)$, then

- $h^m = 1$ for all $h \in G$
- There is some $g \in G$ with $o(g) = m$

Example

- $?? = ?? * ??$
- $\phi(??) = ??$, $\phi(??) = ??$
- $\phi(??) = \phi(??)\phi(??) = ?? * ?? = ??$
- $\lambda(??) = \mathrm{lcm}(??, ??) = ??$
- $\mathbb{Z}_{??}^* \simeq C_{??} \times C_{??}$

Index arithmetic

- $m = p^k$ or $m = 2p^k$
- $\phi(m) = M$
- $\mathbb{Z}_m^* = \langle r \rangle = \left\{ r, r^2, \ldots r^M = [1]_m \right\} \simeq C_M$
- $[a]_m \in \mathbb{Z}_m^*$, i.e. $\gcd(a, m) = 1$
- $a \equiv r^x \mod m$ for a unique x with $1 \leq x \leq M$
- $x = \operatorname{ind}_r(a)$, index of a to base r, or discrete logarithm
- a, b rel prime to m, then $\operatorname{ind}_r(a) = \operatorname{ind}_r(b)$ iff $a \equiv b \mod m$ i.e. if $[a]_m = [b]_m$

Example

- $n = ??$
- $\phi(n) = ??$
- $r = ??$
- $\mathrm{ord}_{??}(r) = ??$
- $?? = ??$
- $\mathrm{ind}_{??}(??) = ??$, etc

Index laws

Theorem

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

- $\mathrm{ind}_r(1) \equiv 0 \mod M$
- $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r(a) + \mathrm{ind}_r(b) \mod M$
- $k \in \mathbb{P}$
- $\mathrm{ind}_r(a^k) \equiv k * \mathrm{ind}_r(a) \mod M$

Just like regular logarithms!

Example

$$
\begin{aligned}
9^x &\equiv 11 \mod 14 \\
\operatorname{ind}_3(9^x) &= \operatorname{ind}_3(11) \\
x * \operatorname{ind}_3(9) &\equiv \operatorname{ind}_3(11) \mod 6 \\
x * 2 &\equiv 4 \mod 6 \\
x &\equiv 2 \mod 3
\end{aligned}
$$

Check: $9^2 = 81 = 5 * 14 + 11 \equiv 11 \mod 14$,
$9^5 \equiv 9(9^2)^2 \equiv 9 * 11^2 \equiv 9 * (-3)^2 \equiv 9 * 9 \equiv 11 \mod 14$.

Definition

- $m, k \in \mathbb{P}$
- $a \in \mathbb{Z}$, $\gcd(a, m) = 1$
- $x^k \equiv a \mod m$ solvable
- Then: a is a kth power residue of m

Example

- $m = 11$, $k = 2$
- $x^4 \equiv 9 \mod 11$ solvable, so 9 is fourth power residue mod 11
- $x^4 \equiv 8 \mod 11$ not solvable, so 8 is not fourth power residue mod 11
- $x^4 \mod 11$ is **??**

Theorem

- $m \in \mathbb{P}$, $M = \phi(m)$, $\mathbb{Z}_m^* = \langle [r]_m \rangle$
- $k \in \mathbb{P}$, $a \in \mathbb{Z}$, $\gcd(a, m) = 1$
- $d = \gcd(k, M)$
- *Then:*

$$x^k \equiv a \mod m$$

solvable iff

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

- *If solvable, precisely d solutions mod m (solutions in $\mathbb{Z}_m^*$)*

Proof.

Translate to

$$k * \mathrm{ind}_r(x) \equiv \mathrm{ind}_r(a) \mod M$$

Write $x \equiv r^y \mod m$, $\mathrm{ind}_r(a) = A$ Get

$$k * y \equiv A \mod M$$

Solvable iff $d|A$. But

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

so this happens iff $\frac{M}{d}A \equiv 0 \mod M$, hence iff

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

□

Example

- $m = 11,\ M = 10,\ k = 4,\ d = 2$
- $$9^5 \equiv 1 \mod 11$$
- $x^4 \equiv 9 \mod 11$ was solvable
- $$8^5 \equiv -1 \mod 11$$
- $x^4 \equiv 8 \mod 11$ was not solvable