Lesson 5
Order and primitive roots modulo a prime

Unit 1
Order and primitive roots

Order of an element modulo p

EXAMPLE Table of powers $a^i[7]$, $a \in \{1, \ldots, 6\}, i = 1, \ldots, 6$.

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

DEFINITION Let p prime, $a \in \mathbb{Z}$ with $p \nmid a$.

The order $\mathrm{ord}_p(a)$ of a modulo p is the minimum $n \geq 1$ such that $a^n \equiv 1[p]$.

EXAMPLE $\mathrm{ord}_7(2) = \mathrm{ord}_7(4) = 3$, $\mathrm{ord}_7(6) = 2$.

Order of an element modulo p

PROPOSITION **Let p prime, $a \in \mathbb{Z}$ with $p \nmid a$ and $n \geq 1$.**

Then $a^n \equiv 1[p] \Leftrightarrow \mathrm{ord}_p(a) \mid n$. In particular $\mathrm{ord}_p(a) \mid p-1$. Fermat

Proof. **If $n = q\,\mathrm{ord}_p(a)$ then $a^n = a^{q\,\mathrm{ord}_p(a)} = \left(a^{\mathrm{ord}_p(a)}\right)^q \equiv 1[p]$.**

Conversely, assume that $a^n \equiv 1[p]$.

Dividing n by $\mathrm{ord}_p(a)$ we have $n = q\,\mathrm{ord}_p(a) + r, 0 \leq r < \mathrm{ord}_p(a)$.

Now $1 \equiv a^n = a^{q\,\mathrm{ord}_p(a)+r} = a^{q\,\mathrm{ord}_p(a)} \cdot a^r [p]$

$$\equiv (a^{\mathrm{ord}_p(a)})^q \cdot a^r [p] \equiv a^r [p]$$

$a^r \equiv 1[p], r < \mathrm{ord}_p(a) \Rightarrow r = 0$. Thus $n = q\,\mathrm{ord}_p(a) : \mathrm{ord}_p(a) \mid n$. $\square$

Order of an element modulo p

COROLLARY Let p prime, $a \in \mathbb{Z}$ with $p \nmid a$.

$$\operatorname{ord}_p(a) \overset{\text{DEF}}{=} \min\{n \geq 1 : \ a^n \equiv 1[p]\}$$

$$= \min\{n \geq 1 : \ a^n \equiv 1[p],\ n \mid p-1\}.$$

PROPOSITION Let p prime. If $g \in \mathbb{F}_p^*$ then $g^x = g^y \Leftrightarrow y \equiv x[\operatorname{ord}_p(g)]$.

Proof. Assume $x \geq y$, dividing $x - y$ by $\operatorname{ord}_p(g)$:

$$x - y = q \operatorname{ord}_p(g) + r, \boxed{0 \leq r < \operatorname{ord}_p(g)}$$

$$g^x = g^{y + q \operatorname{ord}_p(g) + r} = g^y \cdot \left(g^{\operatorname{ord}_p(g)}\right)^q \cdot g^r = g^y \cdot g^r.$$

g is invertible!

$$g^x = g^y \Leftrightarrow \cancel{g^y} = \cancel{g^y} \cdot g^r \Leftrightarrow g^r = 1 \Leftrightarrow r = 0. \ \square$$

Primitive roots

DEFINITION Let p be prime.

USEFUL!

A primitive root of $\mathbb{F}_p$ is any $g \in \mathbb{F}_p^*$ such that $\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$.

EXAMPLE Powers in $\mathbb{Z}/7\mathbb{Z}$.

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

Which elements are primitive roots? 3, 5

THEOREM (Existence of primitive roots)

Let p be a prime. $\mathbb{F}_p$ has at least a primitive root. ADMITTED

How many powers to find a primitive root: first estimate

QUESTION **Let $p \geq 2$ be prime. How many steps to find a primitive root?**

- $|\mathbb{F}_p^* \setminus \{1\}| = p - 2$
- **For each $a \in \mathbb{F}_p^* \setminus \{1\}$ compute $a^2, \ldots, a^{p-2}$: $p - 3$ powers**

In total $N_1(p) = (p-2) \times (p-3) \sim p^2$ as $p \to +\infty$ powers need to be computed.

EXAMPLE

$p = 19$: $N_1(19) = 17 \times 16 = 272$ powers to be computed!

Find the primitive roots

EXAMPLE

1) Write the table of powers in $\mathbb{Z}/5\mathbb{Z}$.

k \ i	1	2	3	4
2	$2^1 = 2$	$2^2 = 4$	$2^3 = 3$	$2^4 = 1$
3	$3^1 = 3$	$3^2 = 4$	$3^3 = 2$	$3^4 = 1$
4	$4^1 = 4$	$4^2 = 1$	$4^3 = 4$	$4^4 = 1$

2) Find the primitive roots in $\mathbb{Z}/5\mathbb{Z}$. 2 3

Primitive roots and order

EXAMPLE **Powers in $\mathbb{Z}/7\mathbb{Z}$. (recall)**

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

The primitive roots are 3, 5.

What is their order modulo 7? 6

The elements that are NOT primitive roots have order < 6.

Primitive roots and their order

THEOREM (characterisation of the primitive roots)

Let p be prime. $g \in \mathbb{F}_p^*$ is a primitive root if and only if $\mathrm{ord}_p(g) = p-1$.

Proof. **Suppose that $\mathrm{ord}_p(g) = p-1$. Claim: $1, g, g^2, \ldots, g^{p-2}$ are distinct.**

If not there are $0 \leq i < j \leq p-2$ and $g^i = g^j$ in $\mathbb{F}_p$. Then $g^{j-i} \equiv 1[p]$.

Thus (Proposition) $p-1 = \mathrm{ord}_p(g) \mid j-i \leq p-2 < p-1$, a contradiction.

Since $g \neq 0$ then $\{1, g, \ldots, g^{p-2}\} = \mathbb{F}_p^*$.

Conversely, assume that $\mathrm{ord}_p(g) = m < p-1$. Then $g^{m+i} = g^i$ for all i so that

$$\#\{1, g, \ldots, g^{p-2}\} = \#\{1, g, \ldots, g^{m-1}\} = m < p-1.$$

Hence $\mathbb{F}_p^* \neq \{1, g, g^2, \ldots, g^{p-2}\}$. $\square$

EXAMPLES

EXAMPLE Let $p > 2$ and g be a primitive root in $\mathbb{F}_p$. Then $g^{\frac{p-1}{2}} = -1$.

Proof. Set $x = g^{\frac{p-1}{2}}$. Then $x^2 = 1$ in $\mathbb{F}_p$.

Then $x = 1$ or $x = -1$. Since $\mathrm{ord}_p(g) = p - 1$ then $x = -1$. $\square$

RECALL Let $p>2$ be a prime. The solutions to $x^2 = 1$ in $\mathbb{F}_p$ are ± 1.

EXAMPLE Let $p > 2$ be prime. If g is a square then g is not a primitive root in $\mathbb{F}_p$.

Indeed, let $g = h^2$. Then $g^{(p-1)/2} = d^{p-1} \equiv 1 \not\equiv -1[p]$.

Powers to find a primitive root: a small refinement

THEOREM (characterisation of the primitive roots)

Let p be prime. $g \in \mathbb{F}_p^*$ is a primitive root if and only if $\mathrm{ord}_p(g) = p-1$.

Let p be prime. In order to check that a is a primitive root one just needs to compute a^i as $i \mid p-1$: it is a primitive root iff for these divisors $i < p-1$ one has $a^i \neq p-1$.

Number of steps:

$N_2(p) = (p-2) \times \#\text{divisors of } (p-1) \text{ strictly less } (p-1) \text{ powers to compute.}$

EXAMPLE

$p = 19$: $\quad p-1 = 18 = 3^2 \times 2$ has $3 \times 2 = 6$ divisors, 5 are < 18.

$N_2(19) = 17 \times 5 = 85$ powers to be computed. About $\frac{1}{4} N_1(19)$.

Unit 2
Primitive roots:
a test

Order of an element modulo p

EXAMPLE **Let $p = 41$. Is 6 a primitive root in $\mathbb{Z}/41\mathbb{Z}$?**

In principle you should check whether $\mathbb{F}_{41}^* = \{6^0, 6^1, \ldots, 6^{39}\}$: about 40 powers.

Enough to check that $\mathrm{ord}_{41}\, 6 = 40$.

Finding a primitive root: an algorithm

LEMMA (a test) **Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.**

Then $g \in \mathbb{F}_p \setminus \{0\}$ is a primitive root if and only if $g^{(p-1)/p_i} \not\equiv 1 [p]$ for $i = 1, \ldots, m$.

Just m tests!

Proof.

Finding a primitive root: an algorithm

TEST Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.

Then $g \in \mathbb{F}_p^*$ is a primitive root if and only if $g^{(p-1)/p_i} \not\equiv 1[p]$ for $i = 1, \ldots, m$.

Just m tests!

ESTIMATE OF m Assume $p - 1 = p_1^{a_1} \cdots p_m^{a_m}$. Then $m \leq \dfrac{\log(p-1)}{\log 2}$.

Finding a primitive root: an algorithm

ALGORITHM Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.

1. $g = 2$.
2. If $g^{(p-1)/p_i} \not\equiv 1$ for all $i = 1, \ldots, m$ then g is a primitive root.
3. If not, back to Step 2 with $g \to g + 1$.

Powers to find a primitive root: second estimate

ALGORITHM Let $p > 2$ be prime and $p - 1 = \prod_{i=1}^{m} p_i^{a_i}$ be the prime decomposition of $p - 1$, with p_i distinct and $a_i \geq 1$ for $i = 1, \ldots, m$.

1. $g = 2$.
2. If $g^{(p-1)/p_i} \not\equiv 1$ for all $i = 1, \ldots, m$ then g is a primitive root.
3. If not, back to Step 2 with $g \to g + 1$.

COROLLARY (Number of powers $N_2(p)$ to find all primitive roots)

Recall: $N_1(p) \sim p^2$ as $p \to +\infty$

$$\text{At most } N_2(p) = (p-2)\frac{\log(p-1)}{\log 2} \overset{*}{\sim} p \log p \text{ as } p \to +\infty \text{ powers.}$$

Finding primitive roots

1. $g = 2$.
2. If $g^{(p-1)/p_i} \not\equiv 1$ for all $i = 1, \ldots, m$ then g is a primitive root.
3. If not, back to Step 2 with $g \to g + 1$.

EXERCISE

43889 is prime. Find a primitive root using at most Mod/PowerMod/factorInteger (Mathematica).

Finding primitive roots

EXAMPLE **Is 3 a primitive root mod. 926510094425921? and 7? use at most Mod/PowerMod/factorInteger (Mathematica)**

Finding primitive roots with Mathematica

PrimitiveRoot[p, k] gives the first primitive root in F_p that is greater than k

PrimitiveRoot[p] : the first prinmitive root in F_p

PrimitiveRootList[p] : all the primitive roots in F_p

```
In[121]:= PrimitiveRoot[37, 5]
Out[121]= 5

In[122]:= PrimitiveRootList[19]
Out[122]= {2, 3, 10, 13, 14, 15}
```

EXAMPLE **43889 is prime. Find a primitive root.**

Unit 3
Finding all the primitive roots knowing one

Number of primitive roots

EXAMPLE

In $\mathbb{Z}/7\mathbb{Z}$ the primitive roots are 3,5: 2 primitive roots.

In $\mathbb{Z}/5\mathbb{Z}$ the primitive roots are 2,4: 2 primitive roots.

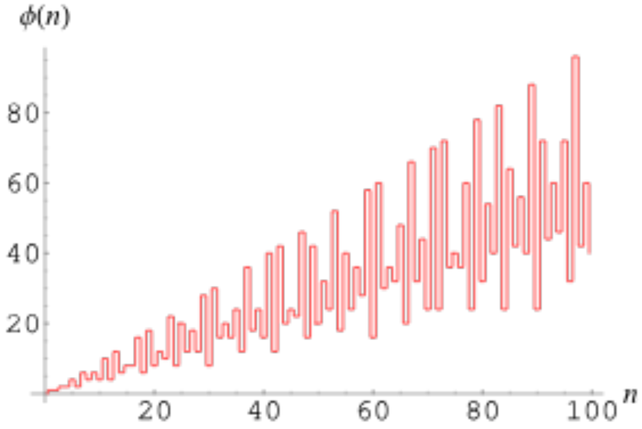
In $\mathbb{Z}/13\mathbb{Z}$ the primitive roots are 2,6, 7, 11: 4 primitive roots.

Number of primitive roots

THEOREM (Characterisation of powers are primitive roots)

Let p be a prime and g be a primitive root of $\mathbb{F}_p$ and $i \in \{1, \ldots, p-2\}$. Then

1. **g^i is a primitive root of $\mathbb{F}_p$ iff $\gcd(i, p-1) = 1$.**
2. **$\mathbb{F}_p$ has $\phi(p-1)$ primitive roots.**



Proof of 1

THEOREM (Characterisation of powers are primitive roots)

Let p be a prime and g be a primitive root of $\mathbb{F}_p$ and $i \in \{1, \ldots, p-2\}$.

1. g^i is a primitive root of $\mathbb{F}_p$ iff $\gcd(i, p-1) = 1$.

2. $\mathbb{F}_p$ has $\phi(p-1)$ primitive roots.

Proof of 1).

Number of primitive roots

EXAMPLE

Knowing that 3 is a primitive root in $\mathbb{Z}/17\mathbb{Z}$, what are all the primitive roots?

Number of powers to find all primitive roots: third estimate (once we have got one)

Let $p \geq 2$ be prime.

How many powers do we need to compute to find all the primitive roots if we have one?

Recall:

$$N_2(p) \overset{*}{\sim} p \log p$$

EXAMPLE

The order of a power

QUESTION Let g be a primitive root in $\mathbb{F}_p$: $\mathbb{F}_p^* = \{1, g, \ldots, g^{p-2}\}$.

What is the order of g^i?

EXAMPLE Is 2 a primitive root in $\mathbb{F}_{13}$?

What is the order of 2^8?

The order of a power

PROPOSITION **Let p be prime, g be a primitive root in $\mathbb{F}_p$ and $i = 1, \ldots, p-2$.**

$$\textbf{Then } \operatorname{ord}_p(g^i) = \frac{p-1}{\gcd(p-1, i)}.$$

First: still a division lemma

RECALL $a \mid bc,\ \gcd(a,b) = 1 \Rightarrow a \mid c.$ **How about if $\gcd(a,b) > 1$?**

LEMMA **Let a, b, c in $\mathbb{Z}$, $a \neq 0$. Then** $a \mid bc \Leftrightarrow \dfrac{a}{\gcd(a,b)} \mid c.$

Proof.

The order of a power

PROPOSITION **Let p be prime, g be a primitive root in $\mathbb{F}_p$ and $i = 1, \ldots, p-2$.**

$$\textbf{Then } \operatorname{ord}_p(g^i) = \frac{p-1}{\gcd(p-1, i)}.$$

COROLLARY

Let g be a primitive root in $\mathbb{F}_p$. Then g^i is . a primitive root iff $\gcd(p-1, i) = 1$.

For how many primes a given number is a primitive root?

QUESTION Let $g \in \mathbb{N}, g \geq 2$. For which primes $p > g$ is g a primitive root in $\mathbb{F}_p$?

EXAMPLE For instance $g = 2$:

For which primes $2 < p < 20$ is 2 a primitive root modulo p?

Artin's conjecture

ARTIN'S CONJECTURE

Proved in 1967 by C. Hooley under the Riemann Hypothesis

If $g \geq 0$ is not a perfect square then

$$\lim_{x \to +\infty} \frac{\#\{p \leq x : \ p \text{ is prime and } g \text{ primitive root in } \mathbb{F}_p\}}{\#\{p : \ p \text{ prime }, p \leq x\}} = C_g > 0$$

$g = 2$: $C_2 = 0.3739558...$

In particular these g are primitive roots for infinitely many primes.

THEOREM (Roger-Heath-Brown, 1985)

There at most two primes that are not primitive roots for infinitely many primes.

EXAMPLE

Thus, among 2, 3, 5 at least one is a primitive root for infinitely many primes.

End of Lesson 5
Order and primitive roots mod. a prime