Cyclic Group: $\boldsymbol{Z_p}^* = \{1, 2, 3, \ldots, \boldsymbol{p}\text{-}1\}$; $\bullet_{\mathbf{mod}\ p}$, $(:_{\mathbf{mod}\ p})$ when division operation is replaced by $\bullet_{\mathbf{mod}\ p}$, by exixting an inverse element in $\boldsymbol{Z_p}^*$:

Let $z \in \boldsymbol{Z_p}^*$, then $z : z_{\mathbf{mod}\ p} = z \bullet z^{-1}{}_{\mathbf{mod}\ p}$.

In group theory, the number of group elements is named as a **group order**.

The order of $\boldsymbol{Z_p}^*$ is $\boldsymbol{p}$-1, i.e. $\text{Ord}(\boldsymbol{Z_p}^*) = |\boldsymbol{Z_p}^*| = \boldsymbol{p}$-1.

When $\boldsymbol{p} = 11$, $\boldsymbol{Z_{11}}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, then $\text{Ord}(\boldsymbol{Z_{11}}^*) = |\boldsymbol{Z_{11}}^*| = 11 - 1 = 10$.

Power Tab. Z_{11}*											
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

If $\boldsymbol{p}$ is **strong prime** then $\boldsymbol{p} = 2\boldsymbol{q} + 1$.
Then $\boldsymbol{q} = (\boldsymbol{p}-1)/2$ is prime as well.
If $\boldsymbol{p} = 11$, then $\boldsymbol{q} = 5$.
$\boldsymbol{G_q} = \boldsymbol{G_5} = \{1, 3, 4, 5, 9\}$.
$|\boldsymbol{G_q}| = \boldsymbol{q}$. $|\boldsymbol{G5}| = 5$.

$3^2 \bmod 11 \neq 1$ & $3^5 \bmod 11 = 1$.
$4^2 \bmod 11 \neq 1$ & $4^5 \bmod 11 = 1$.
$5^2 \bmod 11 \neq 1$ & $5^5 \bmod 11 = 1$.

$9^2 \bmod 11 \neq 1$ & $9^5 \bmod 11 = 1$.

Discrete Exponent Function (10/14)

Notice that there are elements satisfying the following different relations, for example:

$$3^5 = 1 \ \mathbf{mod}\ 11 \text{ and } 3^2 \neq 1 \ \mathbf{mod}\ 11.$$

The set of such elements forms a subgroup of prime order $\boldsymbol{q} = 5$ if we add to these elements the *neutral group element* 1.

This subgroup has a great importance in cryptography we denote by

$$\boldsymbol{G_5} = \{1, 3, 4, 5, 9\}.$$

The multiplication table of $\boldsymbol{G_5}$ elements extracted from multiplication table of $\boldsymbol{Z_{11}}^*$ is presented below.

Multiplication tab. mod 11	G_5				
*	**1**	**3**	**4**	**5**	**9**
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

Values of inverse elements in G_5

$1^{-1} = 1 \bmod 11$
$3^{-1} = 4 \bmod 11$
$4^{-1} = 3 \bmod 11$
$5^{-1} = 9 \bmod 11$
$9^{-1} = 5 \bmod 11$

Exponent tab. mod 11	G_5					
^	**0**	**1**	**2**	**3**	**4**	**5**
1	1	1	1	1	1	1
3	1	3	9	5	4	1
4	1	4	5	9	3	1
5	1	5	3	4	9	1
9	1	9	4	3	5	1

The order $|\boldsymbol{G_5}| = 5$.

Notice that $|\boldsymbol{Z}_{11}^*| = 10 = 1 \cdot 2 \cdot 5$.
Lagrange theorem in Group theory: let $\boldsymbol{G}$ be a group of order N then the order of any subgroup $\boldsymbol{G}_s$ in $\boldsymbol{G}$ divides N, i.e., if $|\boldsymbol{Z}_{11}^*| = 10$, then $|\boldsymbol{G}_5| = 5$ divides 10.

In general, if p is **strong prime** then $p = 2q + 1$, and then $q = (p-1)/2$ is prime as well.
Then $|\boldsymbol{Z}_p^*| = p-1$ and $|\boldsymbol{G}_q| = q$ and q is dividing $p-1$.

Subgroup $\boldsymbol{G}_q$ consist of prime number q elements.
Subgroup $\boldsymbol{G}_q$ consist of elements g' satisfying relation $(g')^q = 1$, i.e. they are of order q except or element 1.

All elements g' in $\boldsymbol{G}_q$ are the generators.
Then g'= is a generator in $\boldsymbol{G}_q$ if and only if (**iff**):
$(g')^2 \bmod 11 \neq 1$ & $(g')^5 \bmod 11 = 1$.

Then subgroup $\boldsymbol{G}_q$ consist of elements g' satisfying relation $(g')^q = 1$, i.e. they are of order q.

$$\mathrm{DEF}_{g',p}(x) = (g')^{x \bmod q} \bmod p = a.$$

In general, if p is **strong prime** then $p = 2q + 1$, and then $q = (p-1)/2$ is prime as well.

To find the subgroup $\boldsymbol{G}_q$ is a difficult problem, in general.

Let p is any prime of order $2^{2048} \sim 2^{700}$.
In Digital Signature Algorithm (DSA) standard this subgroup is presented by prime number q as a Public Parameter.

Example. Let $p = 7 = 2 \cdot 3 + 1$. Then p is a strong prime since $q = 3$ is prime as well.
Find a generators in $\boldsymbol{Z}_7^*$ and subgroup $\boldsymbol{G}_3$ in $\boldsymbol{Z}_7^*$.

^	1	2	3	4	5	0
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1