## Discrete Exponent Function (3/14)

Let $\Gamma$ be the set of generators in $Z_p^* = \{1, 2, 3, \ldots, p\text{-}1\}$ *mod p is defined and /mod p is defined by obtaining the inverse element of divider, e.g. let we want to $a/b$ mod p = $a*(b^{-1})$ mod p.
The secong step is to find $b^{-1}$ mod p.

How to find a generator in $Zp^*$?
In general, it is a hard problem, but using strong prime $p$ and *Lagrange theorem in group theory* the generator in $Z_p^*$ can be found by random search satisfying two following conditions if $p$ is strongprime.

For all $g \in \Gamma$

$$g^q \neq 1 \bmod p; \text{ and } g^2 \neq 1 \bmod p.$$

*Fermat little theorem*: If $p$ is prime then for all integers $i$:

$$i^{p-1} = 1 \bmod p.$$

***Corollaries***: 1. The exponent $p$-1 is equivalent to the exponent 0, since $i^0 = i^{p-1} = 1$ mod $p$-1.

2. Any exponent $e$ can be and should be reduced **mod** ($p$-1), i.e.

$$i^e \bmod p = i^{e \bmod (p-1)} \bmod p.$$

3. All non-equivalent exponents $x$ are in the set $Z_{p-1} = \{0, 1, 2, \ldots, p\text{-}2\}$; +, -, * mod (p-1) and / mod(p-1) with exception.
4. Sets $Z_{p-1}$ and $Z_p^*$ have the same number of elements.

## Discrete Exponent Function (4/14)

In $Z_{p-1}$ addition +, multiplication ∗ and subtraction - operations are realized **mod** ($p$-1).

Subtraction operation ($h$-$d$) **mod** ($p$-1) is replaced by the following addition operation ($h$ + (-$d$)) **mod** ($p$-1)).

Therefore, it is needed to find -$d$ **mod** ($p$-1) such that $d$ + (-$d$) = 0 **mod** ($p$-1), then assume that

$$-d \bmod (p-1) = (p-1-d).$$

Indeed, according to the distributivity property of modular operation

$$(d + (-d)) \bmod (p-1) = (d + (p-1-d) \bmod (p-1) = (p-1) \bmod (p-1) = 0.$$

Then

$$(h-d) \bmod (p-1) = (h + (p-1-d)) \bmod (p-1)$$

## Discrete Exponent Function (5/14)

***Statement***: If greatest common divider between $p$-1 and $i$ is equal to 1, i.e., gcd($p$-1, $i$) = 1, then there exists unique inverse element $i^{-1}$ **mod** ($p$-1) such that $i * i^{-1} \bmod (p\text{-}1) = 1$. This element can be found by *Extended Euclide algorithm* or using *Fermat little theorem*. We do not fall into details how to find $i^{-1}$ **mod** ($p$-1) since we will use the ready-made computer code instead in our modeling.

Division operation / **mod** ($p$-1) of any element in $Z_{p-1}$ by some element $i$ is replaced by multiplication ∗ operation with $i^{-1}$ **mod** ($p$-1) if gcd($i$, $p$-1) = 1 according to the *Statement* above.

To compute $u/i$ **mod** ($p$-1) it is replaced by the following relation $u * i^{-1}$ **mod** ($p$ - 1) since

$$u / i \bmod (p-1) = u * i^{-1} \bmod (p-1).$$

## Discrete Exponent Function (6/14)

***Example 1***: Let for given integers $u$, $x$ and $h$ in $Z_{p-1} = \{0, 1, 2, \ldots, p-2\}$ we compute exponent $s$ of generator $g$ by the expression

$$s = u + xh. \quad \% \text{ this expression mistakenly is computed mod } p$$

Then

$$g^s \bmod p = g^{s \bmod (p-1)} \bmod p.$$

Therefore, $s$ can be and should be computed **mod** $(p-1)$ in advance, to save a multiplication operations, i.e.

$$s = u + xh \bmod (p-1).$$

***Example 2***: Exponent $s$ computation including subtraction by $xr$ **mod** $(p-1)$ and division by $i$ in $Z_{p-1}$ when gcd($i$, $p$-1) = 1.

$$s = (h - xr)i^{-1} \bmod (p-1).$$

Firstly $d = xr \bmod (p-1)$ is computed.
Secondly $-d = -xr \bmod (p-1) = (p-1-d)$ is found.
Thirdly $i^{-1} \bmod (p-1)$ is found.

```
>> d=mod(x*r,p-1);
>> md=mod(-d,p-1)
>> i_m1=mulinv(i,p-1)
% Verification
>> mod(i*i_m1,p-1)
```

And finally exponent $s = (h + (p-1-d))i^{-1} \bmod (p-1)$ is computed. % >> s=mod((h+md)*i_m1,p-1)

## Discrete Exponent Function (7/14)

Referencing to Fermat little theorem and its corollaries, formulated above, the following theorem can be proved.

*Theorem*. If $g$ is a generator in $Z_p^* = \{1, 2, 3, \ldots, p-1\}$ then **DEF** provides the following 1-to-1 of $Z_{p-1} = \{0, 1, 2, \ldots, p-2\}$ to $Z_p^*$.

$$\textbf{DEF}: Z_{p-1} \longrightarrow Z_p^*.$$

Parameters $p$ and $g$ for **DEF** definition we name as Public Parameters and denote by **PP** = ($p$, $g$).

*Example*: Strong prime $p = 11$, $p = 2 * 5 + 1$, then $q = 5$ and $q$ is prime. Then $p-1 = 10$.

$$\textbf{DEF}: \quad Z_{11}^* = \{1, 2, 3, \ldots, 10\} \longrightarrow Z_{10} = \{0, 1, 2, \ldots, 9\}$$

## Discrete Exponent Function (8/14)

The results of any binary operation (multiplication, addition, etc.) defined in any finite group is named *Cayley table* including multiplication table, addition table etc.

Multiplication table of multiplicative group $Z_{11}^*$ is represented below.

| **Multiplication tab. mod** 11 | $Z_{11}^*$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| * | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **1** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **2** | 2 | 4 | 6 | 8 | 10 | 1 | 3 | 5 | 7 | 9 |
| **3** | 3 | 6 | 9 | 1 | 4 | 7 | 10 | 2 | 5 | 8 |
| **4** | 4 | 8 | 1 | 5 | 9 | 2 | 6 | 10 | 3 | 7 |
| **5** | 5 | 10 | 4 | 9 | 3 | 8 | 2 | 7 | 1 | 6 |
| **6** | 6 | 1 | 7 | 2 | 8 | 3 | 9 | 4 | 10 | 5 |

Values of inverse elements in $Z_{11}^*$

| |
|---|
| $1^{-1} = 1 \bmod 11$ |
| $2^{-1} = 6 \bmod 11$ |
| $3^{-1} = 4 \bmod 11$ |
| $4^{-1} = 3 \bmod 11$ |
| $5^{-1} = 9 \bmod 11$ |
| $6^{-1} = 2 \bmod 11$ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **7** | 7 | 3 | 10 | 6 | 2 | 9 | 5 | 1 | 8 | 4 |
| **8** | 8 | 5 | 2 | 10 | 7 | 4 | 1 | 9 | 6 | 3 |
| **9** | 9 | 7 | 5 | 3 | 1 | 10 | 8 | 6 | 4 | 2 |
| **10** | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

| |
|---|
| $7^{-1}= 8 \bmod 11$ |
| $8^{-1}= 7 \bmod 11$ |
| $9^{-1}= 5 \bmod 11$ |
| $10^{-1}= 10 \bmod 11$ |

## Discrete Exponent Function (9/14)

The table of exponent values for $p = 11$ in $Z_{11}^*$ computed **mod** 11 and is presented in table below.
Notice that according to Fermat little theorem for all $z \in Z_{11}^*$, $z^{p-1} = z^{10} = z^0 = 1$ **mod** 11.

| **Exponent tab. mod** 11 | $Z_{11}^*$ | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ^ | **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 |

| |
|---|
| |
| $2^2 \neq 1$ **mod** 11 & $2^5 \neq 1$ **mod** 11 |
| |
| |
| |
| $6^2 \neq 1$ **mod** 11 & $6^5 \neq 1$ **mod** 11 |
| $7^2 \neq 1$ **mod** 11 & $7^5 \neq 1$ **mod** 11 |
| $8^2 \neq 1$ **mod** 11 & $8^5 \neq 1$ **mod** 11 |
| |
| |

## Discrete Exponent Function (10/14)

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

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

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

This subgroup has a great importance in cryptography we denote by

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

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

| **Multiplication tab. mod** 11 | $G5$ | | | | |
|---|---|---|---|---|---|
| * | **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 | $G5$ | | | | | |
|---|---|---|---|---|---|---|
| ^ | **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 |

## Discrete Exponent Function (11/14)

Notice that since $G_5$ is a subgroup of $Z_{11}^*$ the multiplication operations in it are performed **mod** 11.
The exponent table shows that all elements {3, 4, 5, 9} are the generators in $G_5$.
Notice also that for all $\gamma \in \{3, 4, 5, 9\}$ their exponents 0 and 5 yields the same result, i.e.

$$\gamma^0 = \gamma^5 = 1 \bmod 11.$$

This means that exponents of generators $\gamma$ are computed **mod** 5.

This property makes the usage of modular groups of prime order $q$ valuable in cryptography since they

provide a higher-level security based on the stronger assumptions we will mention later.

Therefore, in many cases instead the group $Z_p^*$ defined by the prime (not necessarily strong prime) number $p$ the subgroup of prime order $G_q$ in $Z_p^*$ is used.

In this case if $p$ is strong prime, then generator $\gamma$ in $G_q$ can be found by random search satisfying the following conditions

$$\gamma^q = 1 \bmod p \text{ and } \gamma^2 \neq 1 \bmod p.$$

Analogously in this generalized case this means that exponents of generators $\gamma$ are computed **mod** $q$. In our modeling we will use group $Z_p^*$ instead of $G_q$ for simplicity.

## Discrete Exponent Function (12/14)

Let as above $p$=11 and is strong prime and generator we choose $g$ = 7 from the set $\Gamma$={2, 6, 7, 8}.
Public Parameters are PP=(11,7), Then $DEF_g(x) = DEF_7(x)$ is defined in the following way:

Public Parameters are PP=(11,7), Then $DEF_g(x) = DEF_7(x)$ is defined in the following way:

$$DEF_7(x) = 7^x \bmod 11 = a;$$

$DEF_7(x)$ provides the following 1-to-1 mapping, displayed in the table below.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $7^x \bmod p = a$ | 1 | 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 | 7 | 5 | 2 | 3 |

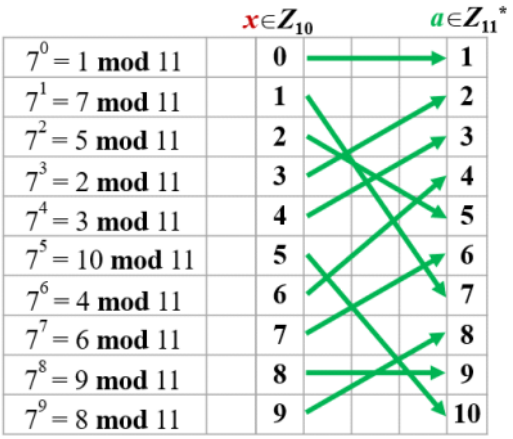
You can see that $a$ values are repeating when $x$ = 10, 11, 12, 13, 14, etc. since exponents are reduced **mod** 10 due to *Fermat little theorem*.

The illustration why $7^x \bmod p$ values are repeating when $x$ = 10, 11, 12, 13, 14, etc. is presented in computations below:
10 mod 10 = 0; 710 = 70 = 1 mod 11 = 1.
11 mod 10 = 1; 711 = 71 = 7 mod 11 = 7.
12 mod 10 = 2; 712 = 72 = 49 mod 11 = 5.
13 mod 10 = 3; 713 = 73 = 343 mod 11 = 2.
14 mod 10 = 4; 714 = 74 = 2401 mod 11 = 3.
etc.

## Discrete Exponent Function (13/14)

C:\Users\Eligijus\Documents\100 MOKYMAS\4 DEF

For illustration of 1-to-1 mapping of $DEF_7(x)$ we perform the following step-by-step computations.



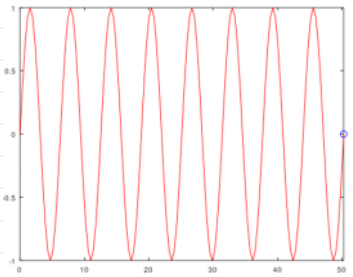

It is seen that one value of $x$ is mapped to one value of $a$.

## Discrete Exponent Function (14/14)

But the most in interesting think is that **DEF** is behaving like a *pseudorandom function*.
It is a main reason why this function is used in cryptography - classical cryptography.
To better understand the pseudorandom behaviour of **DEF** we compare the graph of "regular" **sine** function with "pseudorandom" **DEF** using Octave software.

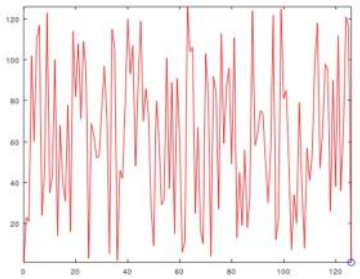
p128sin.m

```
>> p128sin
xrange = 16 * pi;
step = xrange/128;
x = 0:step:xrange;
y = sin(x);
comet(x, y)
```



p128def.m

```
>> p128def    % Strong prime number  p=2*q+1 = 2*63+1
              % q is prime as well
p = 127;
g = 23;
x = 0:p-1;
a = mod_expv(g, x, p);
comet(x, a)
```



$$s = (h - xr)i^{-1} \bmod (p-1).$$

Firstly $d = xr \bmod (p-1)$ is computed:
Secondly $-d = -xr \bmod (p-1) = (p-1-d)$ is found.

Thirdly $i^{-1} \bmod (p-1)$ is found.

And finally exponent $s = (h + (p-1-d))i^{-1} \bmod (p-1)$ is computed.