

Let p is prime, e.g. $p=11$.

$$\mathcal{L}_p^* = \{1, 2, 3, \dots, p-1\} \quad * \bmod p$$

$$\mathcal{L}_{11}^* = \{1, 2, 3, \dots, 10\} \quad * \bmod 11$$

$$\begin{array}{r} -p \mid p \\ \hline 1 \end{array} \quad \begin{array}{r} -p+1 \mid p \\ \hline 1 \end{array}$$

Multiplication Tab \mathbb{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
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

$$2 \cdot 6 = 12 \bmod 11$$

$$\begin{array}{r} 12 \mid 11 \\ \hline 1 \end{array}$$

x	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	12	14	16	18	20
3	0	3	6	9	12	15	18	21	24	27	30
4	0	4	8	12	16	20	24	28	32	36	40
5	0	5	10	15	20	25	30	35	40	45	50
6	0	6	12	18	24	30	36	42	48	54	60
7	0	7	14	21	28	35	42	49	56	63	70
8	0	8	16	24	32	40	48	56	64	72	80
9	0	9	18	27	36	45	54	63	72	81	90
10	0	10	20	30	40	50	60	70	80	90	100

$$\mathcal{L}_{p-1} = \{0, 1, 2, \dots, p-2\} \quad +, -, * \bmod (p-1)$$

$$\mathcal{L}_{10} = \{0, 1, 2, \dots, 9\} \quad \bmod 10$$

Exponent Tab \mathbb{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

$$2^4 \bmod 11 = 16 \bmod 11$$

$$\begin{array}{r} 16 \mid 11 \\ \hline 5 \end{array}$$

$$\leftarrow 2^x \bmod 11$$

$$\leftarrow 6^x \bmod 11$$

$$\leftarrow 7^x \bmod 11$$

$$\leftarrow 8^x \bmod 11$$

$$\Gamma = \{2, 6, 7, 8\}$$

↑
set of
generators
1109

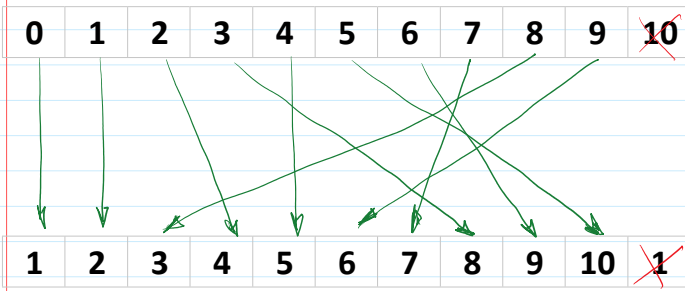
8	1	8	9	6	4	10	3	2	5	1	1 ← 8 mod 11
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

generators
40%

$$\text{DEF}_g : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{11}^* ; 2^x \bmod p = a \in \mathbb{Z}_{11}^*$$

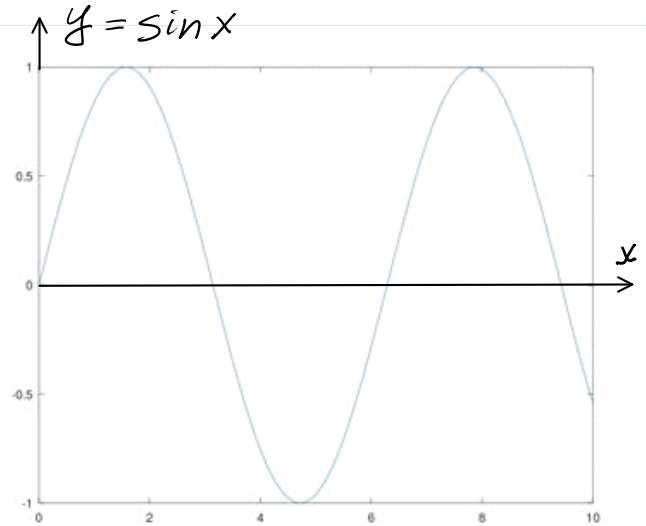
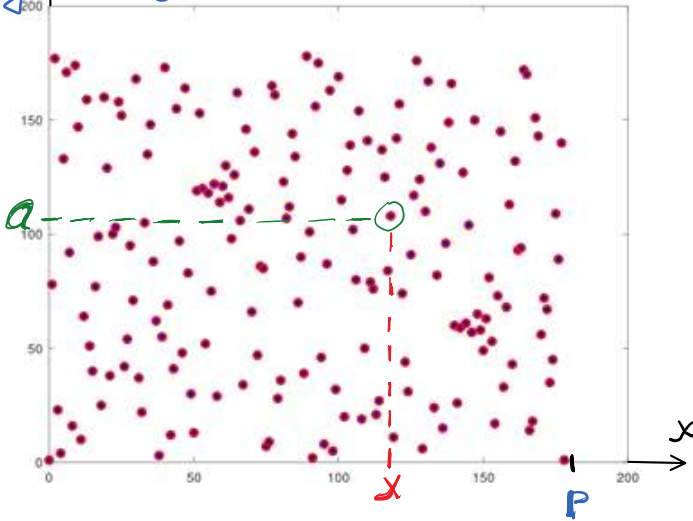
Discrete Exponent Function - DEF:

x	0	1	2	3	4	5	6	7	8	9	10	\mathbb{Z}_{10}
$2^x \bmod p$	1	2	4	8	5	10	9	7	3	6	1	\mathbb{Z}_{11}^*

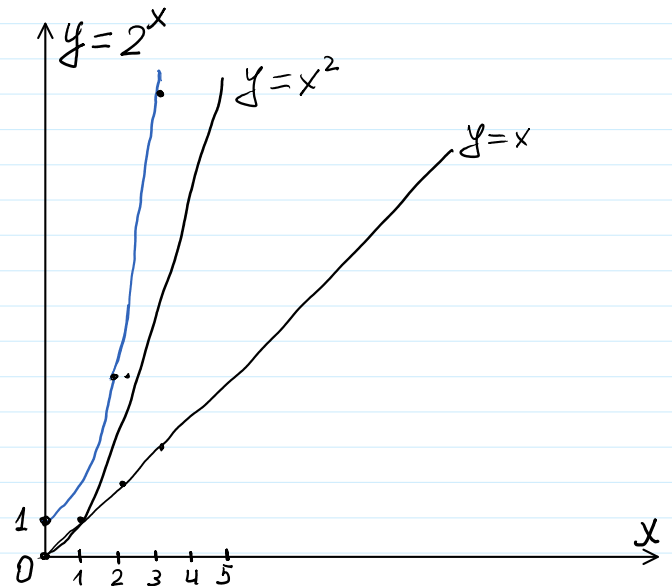
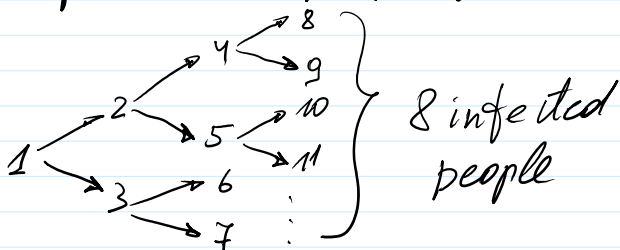


Let p is prime $\Rightarrow \mathbb{Z}_p^* = \{1, 2, 3, \dots, p-1\}$
 $x \in \mathbb{Z}_{p-1} = \{0, 1, 2, 3, \dots, p-2\}$
 $+ \bmod (p-1) \quad - \bmod (p-1)$
 $* \bmod (p-1)$

$$\text{DEF}_g \uparrow a = g^x \bmod p$$



If p is large enough, say $p \sim 2^{2048} \equiv 10^{616}$, then when given p, g, a it is infeasible to find number x .



C.5.3 Finding generators.

We have to look inside \mathbb{Z}_p^* and find a generator. How?

$$p \sim 2^{2048}$$

Even if we have a candidate, how do we test it?

The condition is that g is a generator of \mathbb{Z}_p^* which would take $|\mathbb{Z}_p^*|$ steps to check.

In fact, finding a generator given p is in general a hard problem.

In fact, even checking that g is a generator given p is a hard problem.

But what we can exploit is that is **strong prime** $p=2q+1$ with $q=(p-1)/2$ prime.

Note that the order of the group \mathbb{Z}_p^* is $p-1=2q$. Prime p is called a **strong prime**.

Fact C.23. Say $p=2q+1$ is **strong prime** where $q=(p-1)/2$ is prime. Then g in \mathbb{Z}_p^* is a generator of \mathbb{Z}_p^* iff (if and only if - tada ir tik tada) $g^q \neq 1 \pmod p$ and $g^2 \neq 1 \pmod p$.

```
>> p=genstrongprime(28)
```

```
p = 251487959
```

```
>> q=(p-1)/2
```

```
q = 125743979
```

```
>> isprime(q)
```

```
ans = 1
```

```
>> dec2bin(p)
```

```
>> g=2 → if g is a generator if not
```

```
>> g=3 → " "
```

```
>> g=5 → g was found a generator
```

$a = g^x \pmod p \Rightarrow$

```
>> a = mod_exp(g, x, p)
```



```
ans = ----
```

```
>> mod_exp(g, q, p) % ne 1
```

```
>> mod_exp(g, 2, p) % ne 1
```

Fact C.24. If g is a generator and i is not divisible by q or 2 then g^i is a generator.

Let z be any positive integer (may be greater than p)

$$z \bmod p = \begin{cases} z; & \text{if } z \leq p \\ z \bmod p; & \text{otherwise} \end{cases}$$

$$\begin{array}{r} z + p \\ \vdots \\ \hline r = z \bmod p \end{array}$$

Let $p=11$ and let $z=7$

$$z \bmod p = 7 \bmod 11 = 7$$

$$p + z = -120$$

$$\begin{array}{r} -129 \quad | \quad 11 \\ 11 \quad | \quad 11 \\ \hline \end{array}$$

$$z \bmod p = 7 \bmod 11 = 7$$

$$\text{let } z = 129$$

$$35 \bmod 11 = 8$$

$$\begin{array}{r} 129 \quad | \quad 11 \\ - 11 \quad 11 \\ \hline 19 \\ - 11 \\ \hline 8 \end{array}$$