

Algebraic structures: groups G , semigroups S , fields F, F_p, Z_p , rings R, Z_{p-1} .

$$\begin{array}{llll} \langle G, * \rangle & \langle S, * \rangle & \langle F, \cdot, + \rangle & \langle F, \cdot, + \rangle \\ \langle Z_p^*, \cdot \rangle & \langle Z_{p-1}, \cdot \rangle & \langle Z_p, \cdot, + \rangle & \langle Z_{p-1}, \cdot, + \rangle \\ & \langle Z_{p-1}, + \rangle & & \end{array}$$

$$Z_p^* = \{1, 2, 3, \dots, p-1\} \quad Z_{p-1} = \{0, 1, 2, 3, \dots, p-2\} \cdot \text{mod } p-1; + \text{mod } (p-1)$$

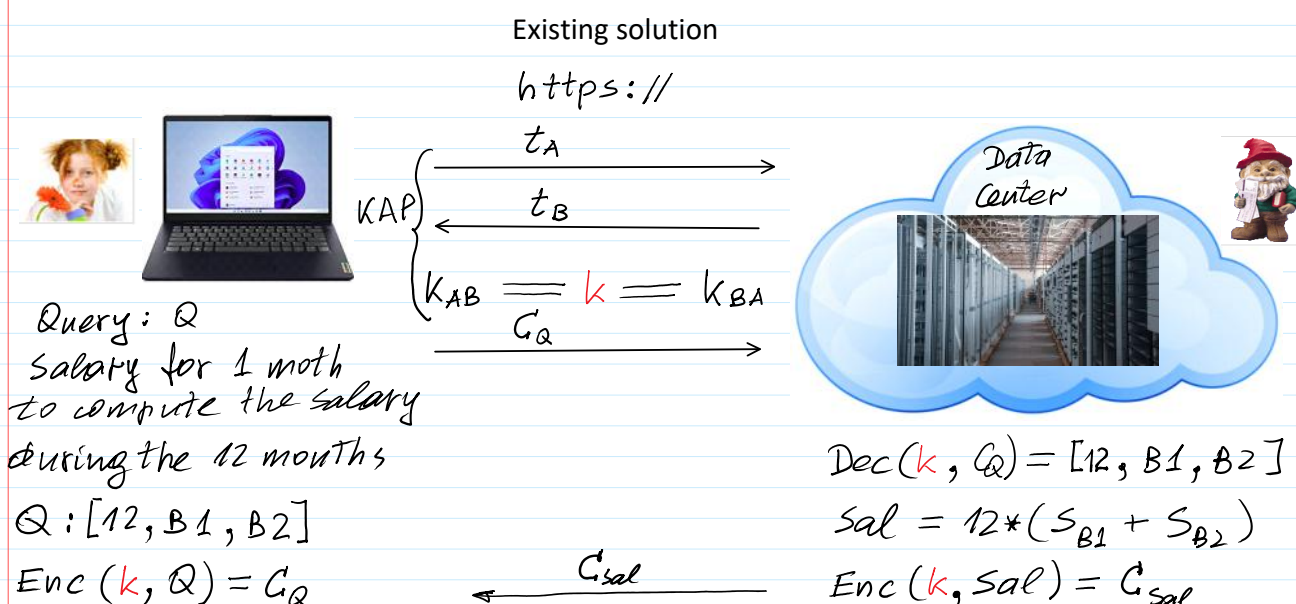
Commutative algebraic structures

Algebraic structure	Number of binary operations	Multiplicative operation $\cdot$	Inverse operation $/$	Additive operation $+$	Inverse operation $-$	Distributivity property $a \cdot (b+c) = a \cdot b + a \cdot c$	Examples
Multiplicative Semigroup	1	Yes	No	No	No	No	$\langle Z_n, \cdot \rangle$ $\cdot \text{mod } n$
Additive Semigroup	1	No	No	Yes	No	No	Set of reals $\mathbb{N}$
Multiplicative Group	1	Yes	Yes	No	No	No	$\langle Z_p^*, \cdot \rangle$
Additive Group	1	No	No	Yes	Yes	No	$\langle Z_n, + \rangle$ $+ \text{mod } n$
Ring	2	Yes	No	Yes	Yes	Yes	$\langle Z_n, \cdot, + \rangle$
Field	2	Yes	Yes	Yes	Yes	Yes	$\langle Z_p, \cdot, + \rangle$

DEF: $Z_{p-1} \rightarrow Z_p^*$, where p is prime.

DEF: is defined by public parameter $PP = (p, g)$

Homomorphic CryptoSystems: Computation with encrypted data in Data Center.



$$\text{Dec}(k, C_{\text{sal}}) = \text{sal}$$

Cloud services



$$\text{Enc}(k, B1) = C_{B1}$$

$$\text{Enc}(k, B2) = C_{B2}$$

$$\text{Enc}(k, 12) = C_{12}$$

$$\text{Dec}(k, C_s) = \text{sal}$$

$$\text{sal} = 12 * (B1 + B2)$$

$$\xrightarrow{C_{B1}, C_{B2}, C_{12}}$$

$$\xleftarrow{C_s}$$

$$C_s = C_{12} * (C_{B1} + C_{B2})$$

Homomorphic encryption

$$F: S_1 \rightarrow S_2; F \in \{\text{surjective, injective, bijective}\}^{1-1 \text{ to } 1}$$

$$\langle S_1, * \rangle, \langle S_2, \bullet \rangle$$

$$\forall x, y \in S_1: F(x * y) = F(x) \bullet F(y) \text{ where } F(x) = a, F(y) = b, a, b \in S_2.$$

If mapping F is bijective (1-to-1) then homomorphism F is isomorphism

Let $\mathbb{R}$ be a field of reals: $\langle \mathbb{R}, \cdot, + \rangle$

$$f: \mathbb{R} \rightarrow \mathbb{R}; f(x) = kx$$

$$1. \text{ check: } f(x_1 + x_2) = k(x_1 + x_2) = kx_1 + kx_2 = f(x_1) + f(x_2)$$

$$2. \text{ check: } f(x_1 \cdot x_2) = k \cdot x_1 \cdot x_2 \neq kx_1 \cdot kx_2 = k^2 \cdot x_1 \cdot x_2$$

$$3. \text{ check: } f(x) = e^x; f: \mathbb{R} \rightarrow \mathbb{R}^+$$

$$f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = f(x_1) \cdot f(x_2)$$

$$\langle \mathbb{R}, + \rangle \rightarrow \langle \mathbb{R}^+, \cdot \rangle$$

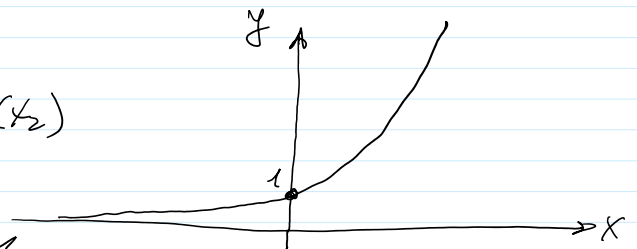
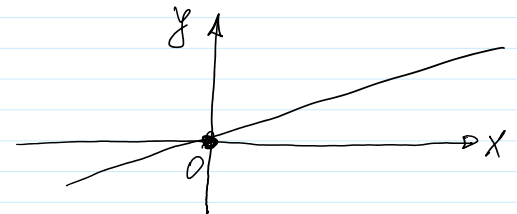
Additively - multiplicative isomorphism.

$$3) \text{ check: } f(x) = g^x \text{ mod } p; \text{ PP} = (p, g)$$

Fermat theorem: If $x \neq 0$, then for $\forall x \in \mathbb{Z}_{p-1}$

$$x^{p-1} = 1 \text{ mod } p$$

$$f: \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^* \text{ and is 1-to-1 (bijective) mapping.}$$



$$x' = 1 \pmod p$$

$\phi: \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^*$ and is 1-to-1 (bijective) mapping.

$$\phi(x_1 + x_2) = g^{x_1 + x_2} \pmod p = g^{x_1} \cdot g^{x_2} \pmod p = \phi(x_1) \cdot \phi(x_2) = a \cdot b \pmod p.$$

Additive ϕ - multiplicative homomorphism.

4 check. $\phi_i(m) = m g^i \pmod p$

$$\phi_i(m_1 + m_2) = (m_1 + m_2) g^i \pmod p = m_1 g^i \pmod p + m_2 g^i \pmod p = \phi_i(m_1) + \phi_i(m_2)$$

$$\phi_i: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*.$$

5. check. $\phi_{i,g}(m) = g^m \cdot g^i \pmod p$

$$\phi_{i,g}(m_1 + m_2) = g^{m_1 + m_2} \cdot g^i \pmod p = g^{m_1} \cdot g^{m_2} \cdot g^i \pmod p \neq \phi_{i,g}(m_1) \cdot \phi_{i,g}(m_2)$$

6. check. $\phi_{i_1,g}(m_1) = g^{m_1} \cdot g^{i_1} \pmod p$; $\phi_{i_2,g}(m_2) = g^{m_2} \cdot g^{i_2} \pmod p$

$$\phi_{i,g}(m_1 + m_2) = g^{m_1 + m_2} \cdot g^i \pmod p = g^{m_1} \cdot g^{m_2} \cdot g^i \pmod p =$$

$$i = (i_1 + i_2) \pmod{(p-1)}$$

$$= g^{m_1} \cdot g^{m_2} \cdot g^{i_1 + i_2} \pmod p = g^{m_1} \cdot g^{i_1} \cdot g^{m_2} \cdot g^{i_2} \pmod p$$

$$= \phi_{i_1,g}(m_1) \cdot \phi_{i_2,g}(m_2).$$

Additively-multiplicative isomorphism if $i = (i_1 + i_2) \pmod{(p-1)}$.

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

```
p = 232702259
```

```
>> pb=dec2bin(p)
```

```
pb = 1101 1101 1110 1100 0001 0011 0011
```

If p - is strong prime, then $p = 2q + 1$,

where q - is prime as well.

An element $g \in \mathbb{Z}_p^*$ is a generator in $\mathbb{Z}_p^*$

if and only if: 1) $g^q \neq 1 \pmod p$

2) $g^2 \neq 1 \pmod p$

```
>> g=2
```

```
g = 2
```

```
>> mod_exp(g,q,p)
```

```
ans = 232702258
```

```
>> mod_exp(g,2,p)
```

```
ans = 4
```

```
>> m1=2000
```

```
m1 = 2000
```

```
>> m2=3000
```

```
m2 = 3000
```

```
>> n1=mod_exp(g,m1,p)
```

```
n1 = 228510651
```

```
>> n2=mod_exp(g,m2,p)
```

```
n2 = 220266692
```

```
>> n12=mod(n1*n2,p)
```

```
n12 = 181510254
```

$$g^{m_1} \cdot g^{m_2} = g^{(m_1 + m_2) \pmod{(p-1)}} \pmod p$$

$$n_{12} = n_1 \cdot n_2 \pmod p = g^{(m_1 + m_2) \pmod{(p-1)}} \pmod p$$

```
>> m1pm2=mod(m1+m2,p-1)
```

```
m1pm2 = 5000
```

```
>> em1pm2=mod_exp(g,m1pm2,p)
```

```
em1pm2 = 181510254
```

Additively-multiplicative homomorphism.

Additively - multiplicative homomorphism.