Octave

WWW.crypto.fmf.ktu.lt

Prisijungimas prie Adobe Connect transliacijų

https://ac.ktu.edu/ https://ac.liedm.net/P120M101

Asmens ident. ⟷ (conditional access) Informac.:
- konfidencialumas
- integralumas
- autentiškumas

} kriptologija

(access rules)

ES parlamentas: 10 G€/m. ⟷ 1000 darbuot.

BBC

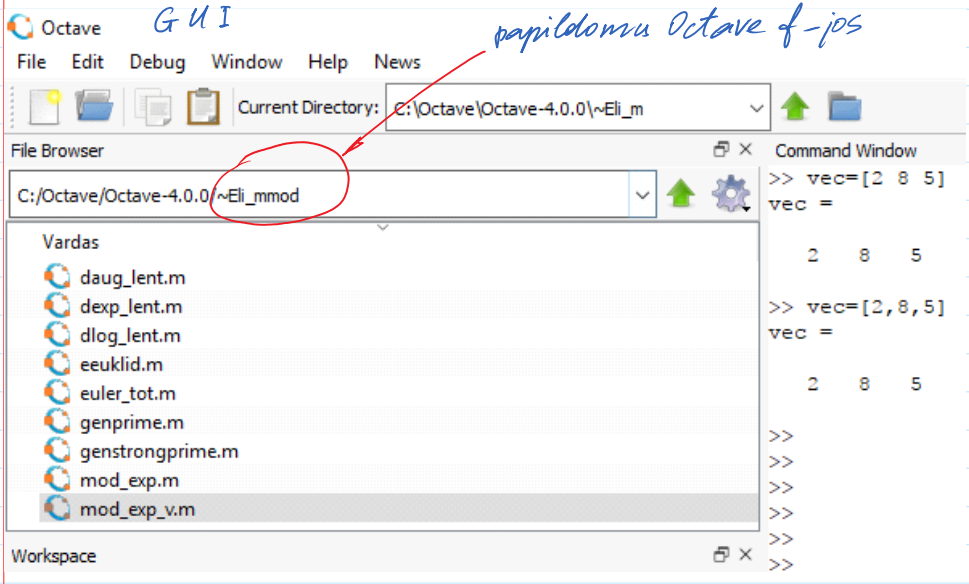
Programav. + Matematika:
- big data
- kriptologija

} → Mag. stud. MA+ → Duomenų analizė ir sauga

imimsociety.net → registracija vardas.pav.@ktu.edu
↓
10 € kredita

Euronews https://www.

http://crypto.fmf.ktu.lt/



$g^e \bmod p$; $g^e \bmod n$

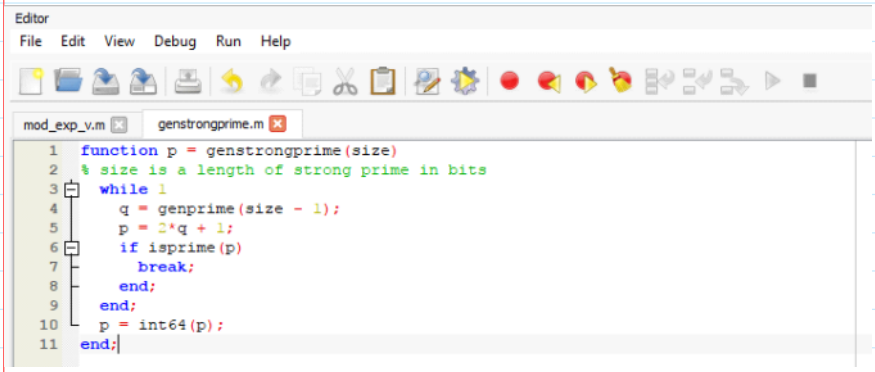
Primes are in P

```
>> daug_lent(17)
ans =

   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16
   2   4   6   8  10  12  14  16   1   3   5   7   9  11  13  15
   3   6   9  12  15   1   4   7  10  13  16   2   5   8  11  14
   4   8  12  16   3   7  11  15   2   6  10  14   1   5   9  13
   5  10  15   3   8  13   1   6  11  16   4   9  14   2   7  12
   6  12   1   7  13   2   8  14   3   9  15   4  10  16   5  11
   7  14   4  11   1   8  15   5  12   2   9  16   6  13   3  10
   8  16   7  15   6  14   5  13   4  12   3  11   2  10   1   9
   9   1  10   2  11   3  12   4  13   5  14   6  15   7  16   8
  10   3  13   6  16   9   2  12   5  15   8   1  11   4  14   7
  11   5  16  10   4  15   9   3  14   8   2  13   7   1  12   6
  12   7   2  14   9   4  16  11   6   1  13   8   3  15  10   5
  13   9   5   1  14  10   6   2  15  11   7   3  16  12   8   4
  14  11   8   5   2  16  13  10   7   4   1  15  12   9   6   3
  15  13  11   9   7   5   3   1  16  14  12  10   8   6   4   2
  16  15  14  13  12  11  10   9   8   7   6   5   4   3   2   1

>> mod_exp(123456789,111511,999)
ans = 702
>> genprime(28)
ans = 262422229
>> p=ans
p = 262422229
>> isprime(p)
ans =  1
```

Stron prime numbers.

1. Choose strong prime *p*; p=2q+1, q is prime.

{5, 7, 11, ~~15~~, 23, 47}




```
>> genstrongprime(20)
>> genstrongprime(20)
ans = 759719
```

patikrinimas: $p = 2q + 1$,

>> genstrongprime(20)
ans = 759719
>> p=ans
p = 759719
>>

patikrinimas: $p = 2q + 1$,
jei q - pirminis
$q = (p-1)/2$

$1K = 2^{10} = 1024$
$1M = 2^{20} > 10^6$
$1G = 2^{30} > 10^9$
$1T = 2^{40} > 10^{12}$

Verification of ***p***
>> q=(p-1)/2
q = 379859

>> isprime(q)
ans = 1
>> factor(q)
ans = 379859
>>

$(O(N))^{1/2}$

1) $P = NP$
2) $N \neq NP$

NP

Outcome ***p*** is strong prime

$17 \bmod 5 = 2$

17 | 5
15 | 3
2

$a = g^x \bmod p$

Algebrinė grupė G : $\langle G, * \rangle$

1. $\forall a, b \in G \rightarrow a * b = c \in G$ Uždarumas
2. $\forall a, b, c \in G \rightarrow (a*b)*c = a*(b*c)$ Asociatyvumas
3. $\exists!$ e - neutr. elem.: $\forall a \in G \rightarrow e * a = a * e = a$ Neutr. elem.
4. $\forall a \in G, \exists!\ \bar{a}^{-1} \rightarrow a * \bar{a}^{-1} = \bar{a}^{-1} * a = e$

Pvz. 1. $\langle G, +_{\bmod p} \rangle$ $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$G = Z_p = \{0, 1, 2, \dots, p-1\}$ // $p \bmod p = 0$

$Z_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$e_+ = 0$

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$e_\cdot = 1$

$\bar{1}^{-1} = 1$ & $\bar{2}^{-1} = 2$
$1 \cdot 1 = 1$ & $2 \cdot 2 = 1$
$\langle Z_3^*, \cdot \rangle$

$Z_3^* = \{1, 2\}$

$Z_{11} = \{0, 1, 2, \ldots, 10\}$; $Z_{11}^* = \{1, 2, 3, \ldots, 10\}$

•	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	3	10	6	2	9	5	1	8	4
	8	5	2	10	7	4	1	9	6	3
	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

>> daug_kent(11)

^	1	2	3	4	5	6	7	8	9	10
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

>> dexp_kent(11)

$Z_{11}^* = \{1, 2, \ldots, 10\}$

g - yra generat., jeigu

$Z_n^* = \{g^i ; i = 0, 1, 2, \ldots, 9\}$

$g^0 = 1$ & $g^{10} = 1$

$0 \equiv 1$

2. Find generator in $Z_p^*=\{1,2,\ldots,p-1\}$, when p is strong prime $p=2q+1$

2.1. Find $q=(p-1)/2$ = 379859

2.2. Choose $1<g<p-1$; For examle g=3

2.3. IF g^q mod p NE 1 AND g^2 mod p NE 1, THEN g is a generator, ELSE repeat 2.2 --> The modular exponent function is required mod_exp(a,n,p)

```
>> genstrongprime(20)
ans = 837107
>> p=ans
p = 837107
>> q=(p-1)/2
q = 418553
>> mod_exp(3,q,p)
ans = 1
>> mod_exp(4,q,p)
ans = 1
>> mod_exp(54,q,p)
ans = 837106
>>
>> mod_exp(54,2,p)
ans = 2916
>>
```

$p = 837107$

$Z^*_{837107} = \{1, 2, 3 \dots, 837106\}$

$g = 54$ – yra generatorius

$Z^*_{837107} = \{54^i ; i = 0, 1, 2, \dots, 837105\}$

Editor

File Edit View Debug Run Help

mod_exp_v.m | genstrongprime.m | *mod_exp.m

```
1  function r = mod_exp(g, n, p)
2  % skaiciuoja r=g^n mod p
3      r = uint64(1);
4      g = uint64(g);
5      n = uint64(n);
6      p = uint64(p);
7      while n > 0
8          if mod(n, 2) ~= 0
9              r = mod(r * g, p);
10         end
11         n = bitshift(n, -1);
12 % Apvalinimas zemyn ( matlab'o funkcija). Pvz. floor(4.99) = 4.
13         g = mod(g * g, p);
14     end
```

$g^n = a$; $a \bmod p$ = liekana, dalijant a iš p

$2^8 \bmod 5 = 256 \bmod 5 = 1$

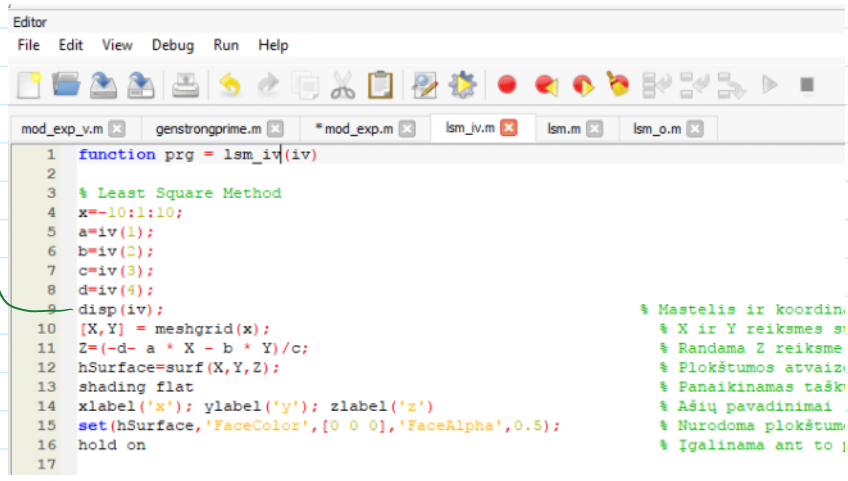
```
>> vec=[2 8 5]
vec =
  2   8   5

>> vec=[2,8,5]
vec =
  2   8   5
```

```
>> vec=[2,8,5]
vec =
   2   8   5


>> mod_exp_v(vec)
 2
   2   8   5
The value of vec(2)is:
 8
Value of vec(2)is: 8
vec(2)is:
 8
vec(2):
 8
ans = 1
>>
```

atsakymas $2^8 \bmod 5$ reikšmė.

```
function r = mod_exp_v(vec)
% skaiciuoja r=g^n mod p
   r = uint64(1);
   disp(vec(1));
   disp(vec);
   disp ("The value of vec(2)is: "), disp(vec(2))
   disp (['Value of vec(2)is: ' num2str(vec(2))])
   disp ('vec(2)is: '); disp(vec(2))
   disp ('vec(2): '); disp(vec(2))
   g = vec(1);
   n = vec(2);
   p = vec(3);
   g = uint64(g);
   n = uint64(n);
   p = uint64(p);
   while n > 0
      if mod(n, 2) ~= 0
         r = mod(r * g, p);
      end
      n = bitshift(n, -1);
% Apvalinimas zemyn (matlab'o funkcija) >>  floor(4.99) = 4.
      g = mod(g * g, p);
   end
```

```
>> iv=[1,1,1,0]
iv =

   1   1   1   0

>> lsm_iv(iv)
   1   1   1   0
A =

   7  -2
  -2  -2
  -5   4

proj =

  -5.33333
   0.66667
   4.66667

>>
```



1.1.step. Student' input : >> pe = [a, b, c, d]

assigned integer values

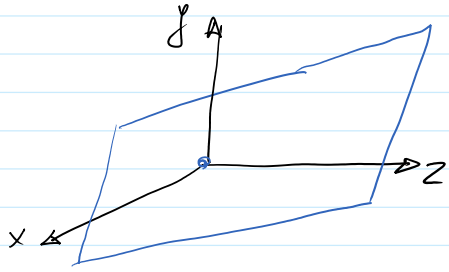
>> pe = [1, 1, 1, 0]

>> lsm_pe(pe)

pe - plane equation crossing zero point

pe == ax + by + cz = 0

1.2. Server returns drawing

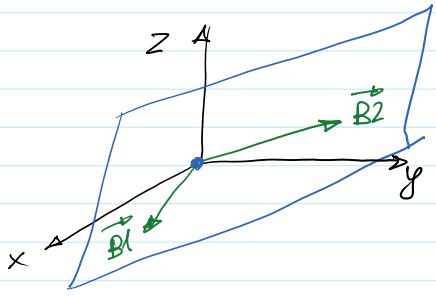


2.1.step. Stud. input $B1 = [b_{1x}, b_{1y}, b_{1z}]$

$B2 = [b_{2x}, b_{2y}, b_{2z}]$

>> lsm_bv(B1, B2) %basic vectors - bv

2.2. Server returns

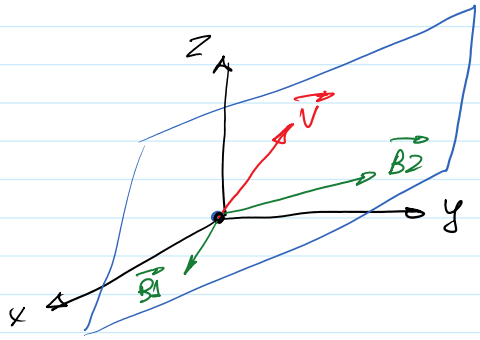


3.1. Stud. input. $V = [v_{1x}, v_{1y}, v_{1z}]$

integers

>> lsm_v(V)

3.2. Server returns



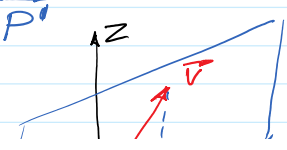
4.1. Student computes proj $\vec{V}$ on the plane $\vec{P}$

Student's input $P' = [P_x, P_y, P_z]$

>> lsm_P(P)

4.2. Server computes proj $\vec{V}$ on the plane $\vec{P'}$

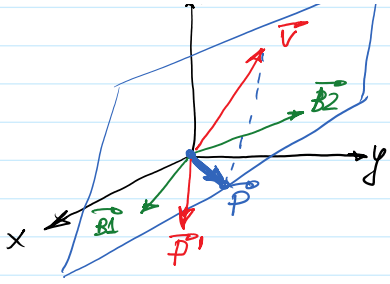
Server returns



server returns

If student computes correctly,

then $\vec{p} = \vec{p}'$



esm_dr(pe, B1, B2, V, p)

1.1. pe, B1 = (0,0,0), B2 = (0,0,0), V = (0,0,0), P = (0,0,0)

① esm_pe(pe)

② esm_bv(pe, B1, B2)

③ esm_v(pe, B1, B2, V)

④