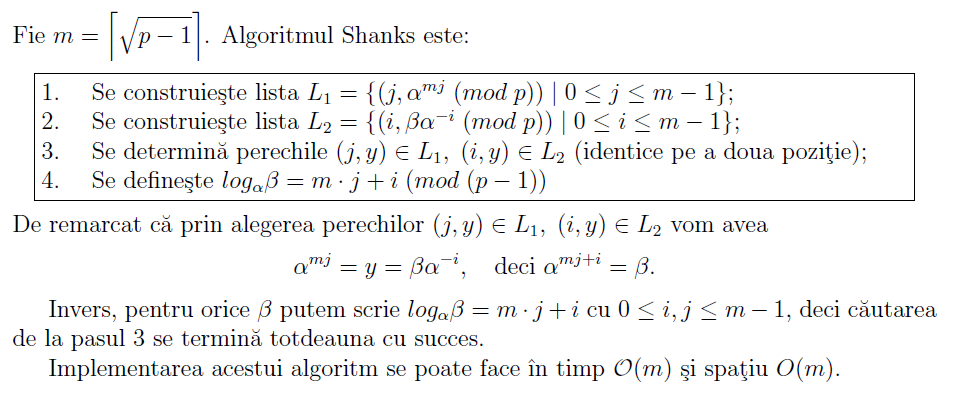
**Algoritmul Shanks**

Algoritmul:



Exemplu:

Fie p = 571, α = 3, β = 233 si m = [23.

Trebuie de determinat log3233mod571

α23 mod 571 = 323 mod 571 = 349

Lista L1 a perechilor (j, 349j mod 571), 0 ≤ j ≤ 22 este:

|  |  |  |  |
| --- | --- | --- | --- |
| (0,1) | (6,556) | (12,225) | (18,51) |
| (1,349) | (7,475) | (13,298) | (19,98) |
| (2,178) | (8,185) | (14,80) | (20,513) |
| (3,454) | (9,42) | (15,512) | (21,314) |
| (4,279) | (10,383) | (16,536) | (22,525) |
| (5,301) | (11,53) | **(17,347)** |  |

3492 mod 571 = 178

|  |  |  |
| --- | --- | --- |
| *i* | *ci* | *z = 1* |
| 1 | 1 | 12 mod 571 = 1 \* 349 mod 571 = 349 |
| 0 | 0 | 3492 mod 571 = 178 |

3493 mod 571 = 454

|  |  |  |
| --- | --- | --- |
| *i* | *ci* | *z = 1* |
| 1 | 1 | 12 mod 571 = 1 \* 349 mod 571 = 349 |
| 0 | 1 | 3492 mod 571 = 178\*349 mod 571 = 454 |

3494 mod 571 = 279

|  |  |  |
| --- | --- | --- |
| *i* | *ci* | *z = 1* |
| 2 | 1 | 12 mod 571 = 1 \* 349 mod 571 = 349 |
| 1 | 0 | 3492 mod 571 = 178 |
| 0 | 0 | 1782 mod 571 = 279 |

3495 mod 571 = 301

|  |  |  |
| --- | --- | --- |
| *i* | *ci* | *z = 1* |
| 2 | 1 | 12 mod 571 = 1 \* 349 mod 571 = 349 |
| 1 | 0 | 3492 mod 571 = 178 |
| 0 | 1 | 1782 mod 571 = 279\*349 mod 571 = 301 |

34917 mod 571 = 347

|  |  |  |
| --- | --- | --- |
| *i* | *ci* | *z = 1* |
| 4 | 1 | 12 mod 571 = 1 \* 349 mod 571 = 349 |
| 3 | 0 | 3492 mod 571 = 178 |
| 2 | 0 | 1782 mod 571 = 279 |
| 1 | 0 | 2792 mod 571 = 185 |
| 0 | 1 | 1852 mod 571 = 536\*349 mod 571 = 347 |

Lista L2 a perechilor (i, 233\*(3i)-1 mod 571), 0 ≤ i ≤ 22 este:

|  |  |  |  |
| --- | --- | --- | --- |
| (0,233) | (6,34) | … | … |
| (1,268) | … | … | … |
| (2,537) | … | … | … |
| **(3,347)** | … | … | … |
| (4,306) | … | … | … |
| (5,102) | … | … | … |

3-1 mod 571 = 381

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 3 | 190 | 1 | 0 | 1 | 381 |
| 3 | 1 | 3 | 0 | 1 | **381** |  |

(32)-1 mod 571 = 365

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 9 | 63 | 4 | 0 | 1 | 508 |
| 9 | 4 | 2 | 1 | 1 | 508 | 365 |
| 4 | 1 | 4 | 0 | 508 | **365** |  |

(33)-1 mod 571 = 423

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 27 | 21 | 4 | 0 | 1 | 550 |
| 27 | 4 | 6 | 3 | 1 | 550 | 127 |
| 4 | 3 | 1 | 1 | 550 | 127 | 423 |
| 3 | 1 | 3 | 0 | 127 | **423** |  |

(34)-1 mod 571 = 141

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 81 | 7 | 4 | 0 | 1 | 564 |
| 81 | 4 | 20 | 1 | 1 | 564 | 141 |
| 4 | 1 | 4 | 0 | 564 | **141** |  |

(35)-1 mod 571 = 47

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 243 | 2 | 85 | 0 | 1 | 569 |
| 243 | 85 | 2 | 73 | 1 | 569 | 5 |
| 85 | 73 | 1 | 12 | 569 | 5 | 564 |
| 73 | 12 | 6 | 1 | 5 | 564 | 47 |
| 12 | 1 | 12 | 0 | 564 | **47** |  |

(36)-1 mod 571 = 206

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***n0*** | ***b0*** | ***q*** | ***r*** | ***t0*** | ***t*** | ***temp*** |
| 571 | 729 | 0 | 571 | 0 | 1 | 0 |
| 729 | 571 | 1 | 158 | 1 | 0 | 1 |
| 571 | 158 | 3 | 97 | 0 | 1 | 568 |
| 158 | 97 | 1 | 61 | 1 | 568 | 4 |
| 97 | 61 | 1 | 36 | 568 | 4 | 564 |
| 61 | 36 | 1 | 25 | 4 | 564 | 11 |
| 36 | 25 | 1 | 11 | 564 | 11 | 553 |
| 25 | 11 | 2 | 3 | 11 | 553 | 47 |
| 11 | 3 | 3 | 2 | 553 | 47 | 412 |
| 3 | 2 | 1 | 1 | 47 | 412 | 206 |
| 2 | 1 | 2 | 0 | 412 | **206** |  |

Raspuns:

Parcurgand aceste 2 liste gasim (17,347)  L1 si (3,347)  L2.

Se poate scrie deci log3233 = 23\*17+3 = **394**

Se poate verifica astfel: 3394 ≡ 233(mod 571)

233 ≡ 233

**Realizarea calculul logaritmului discret modulo este afishat in anexa 2**

**SFARSUIT**

**Calculul logaritmului discret modulo**

**Logarifmul discret**

Source:

import java.util.Scanner;

public class ModulDeGradMare {

private static final int LIMIT = 32000;

public static void main(String[] args) {

int a=0;

int b=0;

int p=0;

try {

System.out.println("Logarifmul discret");

System.out.println(" a ^ x === b (mod p)");

System.out.println("Exemplu: 31 ^ 5 === 3 (mod 29)");

System.out.println("Introduce a : ");

a = (new Scanner(System.in).nextInt());

System.out.println("Introduce b : ");

b = (new Scanner(System.in).nextInt());

System.out.println("Introduce p : ");

p = (new Scanner(System.in).nextInt());

} catch (Exception e) {

System.out.println("Introduse datele incorecte. Numai cifrele pot fi introduse.");

System.exit(1);

}

if (a < 1 || b < 1 || p < 1) {

System.out.println("Datele introduce sunt incorecte. Numai cifrele positive pot fi introduse.");

System.exit(1);

}

int raspuns = aInXModPEqB(a, p, b, LIMIT);

if (raspuns >= 0) {

System.out.println("Raspuns : " + raspuns + "\r\n");

System.out.println(" " + a + " ^ " + raspuns + " === " + b

+ " (mod " + p + ")");

} else {

System.out.println("Raspuns nu a fost gasit.");

}

}

/\*\* a ^ x === b (mod p) \*/

public static int aInXModPEqB(int a, int p, int b, int limit) {

for (int i = 1; i < limit; i++) {

if (pow\_mod(a, i, p) == b)

return i;

}

return -1;

}

/\*\* a ^ k mod n \*/

public static long pow\_mod(long a, long k, long n) {

long b = 1;

while (k > 0) {

if (k % 2 == 0) {

k /= 2;

a = (a \* a) % n;

} else {

k--;

b = (b \* a) % n;

}

}

return b;

}}

**Example:**

Logarifmul discret

a ^ x === b (mod p)

Exemplu: 31 ^ 5 === 3 (mod 29)

Introduce a :

31

Introduce b :

3

Introduce p :

29

Raspuns : 5

31 ^ 5 === 3 (mod 29)