F\*h=G mod q (1)

A mod B= A-r\*B

R=floor(A/B)

From (1):

F\*h-r\*q=G (2)

F\*1-r\*0=F (3)

(2), (3) can be rewritten as vectors:

F\*(h,1)-r(q,0)=(G,F) (4)

F\*1-r\*0=F (5)

F\*h-r\*q=G (6)

F\*(1,h)-r\*(0,q)=(F,G) (7)

V1=(1,h); V2=(0,q) fixed

A1\*v1+a2\*v2=w(a1,a2,v1,v2)

V1=(v11,v12); v2=(v21, v22); V1=(v1(1), v1(2))

A\*(v11,v12)= (A\*v11,A\*v12)

V1+V2=(v11+v21, v12+v22)

V1-V2=(v11-v21, v12-v22)

V1=(1,3); v2=(3,2)

V=v1+v2=(1+3,3+2)=(4,5)

v-v1=v2

v1-v2=(1-3, 3-2)=(-2,1)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 7 |  |  |  |  |  |  |  |  |  |
|  |  | 6 |  |  |  |  |  |  |  |  |  |
|  |  | 5 |  |  |  | v |  |  |  |  |  |
|  |  | 4 |  |  |  |  |  |  |  |  |  |
|  |  | 3 | V1 |  |  |  |  |  |  |  |  |
|  |  | 2 |  |  | V2 |  |  |  |  |  |  |
| V1-v2 |  | 1 |  |  |  |  |  |  |  |  |  |
| -2 | -1 | 0,0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

|  |  |
| --- | --- |
| V11 | V12 |
| V21 | V22 |

B=(v1,v2)

A\*B=w

(a1=1,a2=0)=>(1,2); (a1=2,a2=0)=>(2,4); (a1=3,a2=0)=>(3,6)

(a1=1,a2=1)=>(1+3,2+4)=(4,6); (a1=2,a2=1)=>(2+3,4+4)=(5,8); (a1=3,a2=1)=>(3+3,6+4)=((6,10)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Y |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  | xx |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  | xx |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |
| 6 |  |  | xx | xx |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |
| 4 |  | xx | xx |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |
| 2 | xx |  |  |  |  |  |  |  |  |
| 1. |  |  |  |  |  |  |  |  |  |
| 0,0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | x |

V=(v1,v2) Euclidean norm; n=2;

V1\*v2 dot product or scalar product

V1=(v11,v12); V2=(v21,v22);

(V1,v2)=v11\*v21+v12\*V22+…+v1n\*v2n

(v11\*v21+v12\*V22)/(v11^2+v12^2)

Q=100; f=7<sqrt(q/2)=sqrt(50); sqrt(q/4)=sqrt(25)<g=6<sqrt(q/2)

F=7; g=6; q=100;