Attaque des générateurs congruentiels linéaires

```
(x0,x1,x2,x3,x4)=577,114,910,666,107
```

```
multiple1=(x3-x2)*(x1-x0)-(x2-x1)^2; multiple1
```

```
    -520644
```

```
multiple2=(x4-x3)*(x2-x1)-(x3-x2)^2;multiple2
```

```
    -504500
```

```
gcd(multiple1,multiple2)
```

```
    4036
```

```
factor(4036)
```

```
    2^2 * 1009
```

```
# Le modulo est donc parmi 1009, 2018 ou 4036
# On essaie d'abord 4036
m = 4036
```

```
# On calcule l'inverse du facteur (x_n-x_{n+1}) modulo m
inv=1/Mod(x0-x1,m); inv
```

```
    1787
```

```
# On résout le système modulo m
(a,b)=(Mod( (x1-x2)*inv, m) , Mod( (-x1^2+x0*x2)*inv, m) );a,b
```

```
    (2256, 2030)
```

```
# On vérifie que le modulo était correct ?
a*x0+b,a*x1+b,a*x2+b,a*x3+b,a*x4+b
```

```
    (114, 910, 666, 3134, 1262)
```

```
# Le modulo est parmi 1009, 2018 or 4036
# On essaie maintenant 1009
m = 1009
inv=1/Mod(x0-x1,m)
(a,b)=(Mod( (x1-x2)*inv, m) , Mod( (-x1^2+x0*x2)*inv, m) );a,b
```

```
    (238, 12)
```

```
# On vérifie que l'on a trouvé le modulo et les facteurs corrects du
générateur
a*x0+b,a*x1+b,a*x2+b,a*x3+b,a*x4+b
```

```
    (114, 910, 666, 107, 253)
```

```

```