Algorithm-1.3-Shanks' algorithm for extracting a square root of a modulo p-page 19

Ta the Anh

6/25/2020

```
def Legendre(n,p):
    return pow(n, (p - 1) // 2, p)

def Shanks(a,p):
    n=2
    while Legendre(n,p) != -1 :
        n = ZZ.random_element(2,p-1)
    q = p - 1
    e = 0
    while q%2 == 0:
        q = q // 2
        e = e + 1
    y = pow(n, q, p)
    r = e
    x = pow(a, (q-1)//2, p)
    b = (a*x^2) % p
    x = (a*x) % p
    while b%p != 1:
        m=0
        while pow(b,2**m,p):
            m = m+1
        t = pow(y,2**(r-m-1),p)
        y = pow(t,2,p)
        r = m
        x = (x*t) % p
        b = (b*y) % p
    return x
Shanks(5,19)
```

```
9
```