1 Problem statement

Implement the algorithm for solving systems of congruences.

2 Algorithms

2.1 Euclid's extended algorithm

Ensure: $c = gcd(a, b)$ and $u, v \in \mathbb{Z}, au + bv = c$

procedure EUCLID(a,b)
  $u_2 \leftarrow 1$
  $u_1 \leftarrow 0$
  $v_2 \leftarrow 0$
  $v_1 \leftarrow 1$
  while $b > 0$ **do**
    q $\leftarrow \lfloor a/b \rfloor$
    r $\leftarrow a - qb$
    u $\leftarrow u_2 - qu_1$
    v $\leftarrow v_2 - qv_1$
    a $\leftarrow$ b
    b $\leftarrow$ r
    $u_2 \leftarrow u_1$
    $u_1 \leftarrow u$
    $v_2 \leftarrow v_1$
    $v_1 \leftarrow v$
    d $\leftarrow$ a
    u $\leftarrow u_2$
    v $\leftarrow v_2$
  end while
  euclid $\leftarrow$ a
end procedure

2.2 Key generation

procedure GENERATE_KEY
  p $\leftarrow$ random_prime_number
  g $\leftarrow$ generator_of_$\mathbb{Z}_p$
  a $\leftarrow$ random_integer $\in 1, p - 2$

public_key ← p,g,g^a
private_key ← a
end procedure

2.3 Encryption

procedure GENERATE_KEY(p, g, g^a,m)
k ← random_integer $\in 1, p - 2$
$\alpha \leftarrow g^k \mod p$
$\beta \leftarrow , \cdot (g^a)^k \mod p$
c ← (α, β)
end procedure

2.4 Decryption

procedure DECRYPTION(p, g, g^a,a, α, β)
m ← $\alpha^{-a} \cdot \beta \mod p$
end procedure