

CSCI 162/284 Cryptography: Euclidean Algorithm for the Multiplicative Inverse

The euclidean algorithm for the gcd of two elements may be extended to determine the multiplicative inverse as follows. If the gcd of two elements is one, that is, if $\gcd(m, a) = 1$, then the euclidean algorithm can be modified to provide integers s and t such that $sm + ta = 1$. $t \bmod m$ is then the multiplicative inverse of $a \bmod m$.

1 Modified Euclidean Algorithm

The modified euclidean algorithm is as follows:

```

ModifiedEuclidean(m, a) /* m > a */
    /* Part I: Keep track of the quotient */
    i := 0 /* Initialize */
    (X0, Y0) := (m, a) /* Initialize */
    while (Yi ≠ 0) /* While GCD has not been found */
        {
            qi = ⌊ Xi / Yi ⌋ /* Keep track of quotient */
            (Xi+1, Yi+1) := (Yi, Xi rem Yi) /* Recursion step */
            i := i + 1
        }
    i := i - 1
    X = Yi /* Keep value of Yi, it is GCD */

    /* Part II: Go back up */
    (s, t) := (0, 1) /* Initialize */
    while (i ≠ 0) /* While not at top */
        {
            i := i - 1
            (s, t) := (t, s - t × qi) /* Recursion step */
        }
    return(X, (s,t))

```

Example Use the euclidean algorithm to determine $2652^{-1} \bmod 8855$. The first round gives:

$$\begin{aligned}
 (X_0, Y_0, i, q_0) &= (8855, 2652, 1, 3) \\
 (X_1, Y_1, i, q_1) &= (2652, 899, 1, 2) \\
 (X_2, Y_2, i, q_2) &= (899, 854, 2, 1) \\
 (X_3, Y_3, i, q_3) &= (854, 45, 3, 18) \\
 (X_4, Y_4, i, q_4) &= (45, 44, 4, 1)
 \end{aligned}$$

$$\begin{aligned}(X_5, Y_5, i, q_5) &= (44, 1, 5, 44) \\ (X, Y, i) &= (1, 0, 6)\end{aligned}$$

Going back up:

$$\begin{aligned}(X_0, Y_0, i, q_0, s, t) &= (8855, 2652, 1, 3, 59, -20 - (59)(3) = -197) \\ (X_1, Y_1, i, q_1, s, t) &= (2652, 899, 1, 2, -20, 19 - (-20)(2) = 59) \\ (X_2, Y_2, i, q_2, s, t) &= (899, 854, 2, 1, 19, -1 - (19)(1) = -20) \\ (X_3, Y_3, i, q_3, s, t) &= (854, 45, 3, 18, -1, 1 - (-1)(18) = 19) \\ (X_4, Y_4, i, q_4, s, t) &= (45, 44, 4, 1, 1, 0 - (1)(1) = -1) \\ (X_5, Y_5, i, q_5, s, t) &= (44, 1, 5, 44, 0, 1) \\ (X, Y, i) &= (1, 0, 6) \\ \text{return}(1, 59, -197)\end{aligned}$$

Hence $59 \times 8855 + (-197) \times 2652 = 1$. Hence $2652^{-1} \text{ mod } 8855 = -197 \text{ mod } 8855 = 8658 \text{ mod } 8855$.

2 Correctness of Algorithm

We know that the above algorithm returns the correct gcd . We show that it returns the correct values of s and t .

Theorem: $(X, (s, t))$ returned by $\text{ModifiedEuclidean}(m, a)$ are such that $X = sm + ta$.

Proof: We show that $s_k \times X_k + t_k \times Y_k = \text{gcd}(X_k, Y_k)$ for $0 \leq k \leq N - 1$ by induction. Hence, in particular, this implies that $s_0 \times X_0 + t_0 \times Y_0 = \text{gcd}(X_0, Y_0)$, which, we have shown, is X . Hence, this implies that $sm + ta = X$

Base Case: $s_{N-1} \times X_{N-1} + t_{N-1} \times Y_{N-1} = 0 \times X_{N-1} + 1 \times Y_{N-1} = Y_{N-1} = \text{gcd}(X_{N-1}, Y_{N-1})$. As $Y_{N-1} | X_{N-1}$. Hence the inductive hypothesis is true for $k = N - 1$.

Inductive Case: Assume the hypothesis is true for $k = n$, such that $1 \leq n \leq N - 1$. Then,

$$\begin{aligned}s_n \times X_n + t_n \times Y_n &= \text{gcd}(X_n, Y_n) \\ \Rightarrow s_n \times Y_{n-1} + t_n \times (X_{n-1} - q_{n-1} \times Y_{n-1}) &= \text{gcd}(X_{n-1}, Y_{n-1}) \\ \Rightarrow t_n \times X_{n-1} + (s_n - t_n q_{n-1}) \times Y_{n-1} &= \text{gcd}(X_{n-1}, Y_{n-1}) \\ \Rightarrow s_{n-1} \times X_{n-1} + t_{n-1} \times Y_{n-1} &= \text{gcd}(X_{n-1}, Y_{n-1})\end{aligned}$$

This implies the hypothesis is true for $k = n - 1$. Hence it is true for $k = 0$.

□