Extended Euclidean Algorithm and Fast Exponentiation

Lab 2: RSA

Euclidean Algorithm

$$
\begin{aligned}
a &= q_1 b + r \\
r_0 &= q_1 r_1 + r_2 \\
r_1 &= q_2 r_2 + r_3 \\
r_2 &= q_3 r_3 + r_4 \\
&\vdots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2} \\
&\vdots
\end{aligned}
$$

Euclidean Algorithm

$$
\begin{aligned}
a &= q_1 b + r \\
r_0 &= q_1 r_1 + r_2 \\
r_1 &= q_2 r_2 + r_3 \\
r_2 &= q_3 r_3 + r_4 \\
&\vdots \\
r_i &= q_{i+1} r_{i+1} + r_{i+2} \\
&\vdots
\end{aligned}
\qquad
\begin{aligned}
r_2 &= r_0 - q_1 r_1 \\
r_3 &= r_1 - q_2 r_2 \\
r_4 &= r_2 - q_3 r_3 \\
&\vdots \\
r_{i+1} &= r_{i-1} - q_i r_i \\
&\vdots
\end{aligned}
$$

Extended Euclidean Algorithm

Define two new sequences: s_i and t_i as follows:

$$\begin{aligned} s_0 &= 1 & \qquad t_0 &= 0 \\ s_1 &= 0 & \qquad t_1 &= 1 \\ s_{i+1} &= s_{i-1} - q_i s_i & \qquad t_{i+1} &= t_{i-1} - q_i t_i \end{aligned}$$

Extended Euclidean Algorithm

Claim: For $i \geq 0$, $r_i = s_i a + t_i b$

$$
\begin{array}{lcll}
r_0 & = & s_0 a + t_0 b? & \text{YES!} \qquad r_0 = a = 1 \cdot a + 0 \cdot b \\
r_1 & = & s_1 a + t_1 b? & \text{YES!} \qquad r_1 = b = 0 \cdot a + 1 \cdot b \\
r_i & = & s_i a + t_i b? & \text{YES!}
\end{array}
$$

$$
\begin{aligned}
r_{i+1} &= r_{i-1} - r_i q_i = (a s_{i-1} + b t_{i-1}) - (a s_i + b t_i) q_i \\
&= (a s_{i-1} - a s_i q_i) + (b t_{i-1} - b t_i q_i) = a s_{i+1} + b t_{i+1}
\end{aligned}
$$

Extended Euclidean Algorithm

Define two new sequences: s_i and t_i as follows:

$$\begin{aligned} s_0 &= 1 & \qquad t_0 &= 0 \\ s_1 &= 0 & \qquad t_1 &= 1 \\ s_{i+1} &= s_{i-1} - q_i s_i & \qquad t_{i+1} &= t_{i-1} - q_i t_i \end{aligned}$$

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while   y ≠ 0
        r := x mod y
        x := y
        y := r
return x {gcd(a,b) is x}
```

- In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.