Lecture 14: Extended GCD Algorithm
Objective

- The objective of this lecture is to study the GCD and the Extended GCD algorithms.
- Furthermore, we shall find another technique to find the multiplicative inverse of \( X \in \mathbb{Z}_p^* \) in the group \((\mathbb{Z}_p^*, \times)\).
Given integers $A$ and $B$, our objective is to find the GCD of $A$ and $B$

We shall rely on the following identity to calculate the GCD efficiently

$$\text{gcd}(A, B) = \text{gcd}(B, R),$$

where $R$ is the remainder of the division of $A$ by $B$ (in previous lectures, we already saw an efficient algorithm for division).

Why is this algorithm efficient? Because, if $B \leq A$, then the number of bits needed to represent $(B, R)$ is (at least) one less than the number of bits needed to represent $(A, B)$.

What is the base case of this algorithm? If $B = 0$, then we know that $A = \text{gcd}(A, B)$.

Let us write the code for this recursive algorithm

```python
GCD(A, B):
    If $B == 0$ : return $A$
    else : return GCD($B, A\%B$)
```
We shall now unroll this recursion to make the code more efficient.

\[
\text{GCD}(A, B): \\
\begin{align*}
\text{While } B \neq 0 : \quad & \quad \text{R} = A \% B \\
& \quad A = B \\
& \quad B = R \\
\end{align*}
\]

\begin{itemize}
  \item return A
\end{itemize}
The extended GCD of \((A, B)\) returns three integers \((G, \alpha, \beta)\) such that

\[
G = \gcd(A, B) \quad \text{and} \quad G = \alpha \cdot A + \beta \cdot B.
\]

Note that we can use the extended GCD algorithm to invert \(X \in \mathbb{Z}_p^*\), where \(p\) is a prime. Observe that \((G, \alpha, \beta) = \text{XGCD}(X, p)\) shall satisfy the following constraints

\[
G = 1 \quad \text{and} \quad G = \alpha \cdot X + \beta \cdot p.
\]

Taking \(\mod p\) on both side of the equality, we get that \(\alpha \mod p\) is the multiplicative inverse of \(X\) in the group \((\mathbb{Z}_p^*, \times)\).

Let us use the template of the recursive GCD algorithm to implement the recursive extended GCD algorithm.
Again, we shall use $B = 0$ as the base case. In this case we have $G = \text{gcd}(A, B) = A$, and we can express $G = 1 \cdot A + 0 \cdot B$. Therefore, the base case should return $(G, \alpha, \beta) = (A, 1, 0)$

Now, let us consider the recursive step. Suppose from the recursive call $\text{XGCD}(B, R)$ returns $(G, \alpha', \beta')$. We need to find what $\text{XGCD}(A, B)$ returns. Observe that recursively, we have the guarantee that $G = \alpha' \cdot R + \beta' \cdot R$. Note that $R = A - \gamma \cdot B$. Substituting this expression of $R$, we get

$$G = \alpha' \cdot B + \beta' \cdot (A - \gamma \cdot B) = \beta' \cdot A + (\alpha' - \gamma \beta') \cdot B.$$ 

Therefore, we can set $\alpha = \beta'$ and $\beta = \alpha' - \gamma \beta'$. So, $\text{XGCD}(a, b)$ should return $(G, \beta', \alpha' - \gamma \beta')$. 
Here, we write down the code.

XGCD\((A, B)\):

- If \(B == 0\) : return \((A, 1, 0)\)
- Else :
  - \(R = A \mod B\)
  - \((G, \alpha', \beta') = \text{XGCD}(B, R)\)
  - \(\gamma = (A - R) / B\)
  - return \((G, \beta', \alpha' - \gamma \cdot \beta')\)
We shall implement the program stack ourselves
Let us do this in two steps. First, we shall write the code that implements the recursive calls made by the GCD calculations. In the second part, we shall use the information on the return path up.

The first part of the code proceeds as follows

\[
\text{XGCD}(A, B) : \\
\begin{align*}
\text{stack} &= [] \\
\text{While } B \neq 0 : \\
&\quad R = A \% B \\
&\quad M = (A - R) / B \\
&\quad \text{stack}.append([M, NULL, NULL]) \\
&\quad A = B \\
&\quad B = R \\
&\quad \text{stack}.append([\infty, 1, 0]) \\
\text{gcd} &= A
\end{align*}
\]
At this point, let us pause and understand what our data structure looks like. Suppose we choose the notation that 

\((m_i, \alpha_i, \beta_i)\) are the values of \((m, \alpha, \beta)\) in the \(i\)-th depth recursion.

<table>
<thead>
<tr>
<th>(i = 0)</th>
<th>(i = 1)</th>
<th>(i = 2)</th>
<th>(\ldots)</th>
<th>(i = d - 2)</th>
<th>(i = d - 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m_1)</td>
<td>(m_2)</td>
<td>(m_3)</td>
<td>(\ldots)</td>
<td>(m_{d-1})</td>
<td>(m_d = \infty)</td>
</tr>
<tr>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>(\ldots)</td>
<td>NULL</td>
<td>1</td>
</tr>
<tr>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>(\ldots)</td>
<td>NULL</td>
<td>0</td>
</tr>
</tbody>
</table>

Now, we run an iterator \(i \in \{d - 2, d - 3, \ldots, 0\}\) and update the entries \(\alpha_i\) and \(\beta_i\).
Here is the remaining part of the code

··· Continued from the first part ···

- $d = \text{len}(\text{stack})$
- for $i$ in $\{d - 2, d - 3, \ldots, 0\}$ :
  - $\text{stack}[i][1] = \text{stack}[i + 1][2]$
  - $\text{stack}[i][2] = \text{stack}[i + 1][1] - \text{stack}[i][0] \cdot \text{stack}[i + 1][2]$
- Return $(\text{gcd}, \text{stack}[0][1], \text{stack}[0][2])$
Multiplicative Inverse in $\mathbb{Z}_p^*$

- Let $X \in \mathbb{Z}_p^*$, where $p$ is a prime
- Therefore, we have $\gcd(X, p) = 1$
- By the extended GCD algorithm, we can find integers $\alpha$ and $\beta$ such that $1 = \alpha \cdot X + \beta \cdot p$
- Now, we take $\mod p$ on both sides of the equality to obtain
  \[ 1 = (\alpha \mod p) \cdot x + 0 \mod p. \]
- That is, we have $(\alpha \mod p)$ as the multiplicative inverse of $X$ in the group $(\mathbb{Z}_p^*, \times)$
- This computation can be performed by taking $\mod p$ in the stack[i][1] and stack[i][2] evaluations in the extended GCD algorithm