# COMP8760

Lecture 5

Worksheet for Practice

Sanjay Bhattacherjee

1. **Extended Euclidean Algorithm**
   Fill in the blanks.

   (a) We define the *floor* notation $\lfloor x \rfloor$ as the *largest integer smaller than or equal to $x$*. So,

$$\begin{aligned}
\lfloor 20 \rfloor &= ______ \\
\left\lfloor \tfrac{20}{7} \right\rfloor &= ______ \\
\left\lfloor \tfrac{22}{7} \right\rfloor &= ______ \\
\left\lfloor \tfrac{22}{27} \right\rfloor &= ______ \\
\left\lfloor \tfrac{-22}{7} \right\rfloor &= ______ \\
\left\lfloor \tfrac{-20}{7} \right\rfloor &= ______ \\
\lfloor -20 \rfloor &= ______
\end{aligned}$$

   (b) Find $\gcd(24, 21)$:

| | | |
|---|---|---|
| Input: | $a \leftarrow$ ______, $b \leftarrow$ ______ | |
| Initialisation: | | |
| $r' \leftarrow 24, s' \leftarrow 1, t' \leftarrow 0,$ | $r' \leftarrow s' \times a + t' \times b = 1 \times 24 + 0 \times 21$ | = ______ |
| $r \leftarrow 21, s \leftarrow 0, t \leftarrow 1,$ | $r \leftarrow s \times a + t \times b = 0 \times 24 + 1 \times 21$ | = ______ |
| Iterations: | | |
| $q$ | $\leftarrow$ ______ | = ______ |
| $r$ | $\leftarrow$ ______ | = ______ |
| $s$ | $\leftarrow$ ______ | = ______ |
| $t$ | $\leftarrow$ ______ | = ______ |
| $s \cdot a + t \cdot b$ | = ______ | = ______ |
| | | |
| $q$ | $\leftarrow$ ______ | = ______ |
| $r$ | $\leftarrow$ ______ | = ______ |
| $s$ | $\leftarrow$ ______ | = ______ |
| $t$ | $\leftarrow$ ______ | = ______ |
| $s \cdot a + t \cdot b$ | = ______ | = ______ |
| Final: | $d \leftarrow r', x \leftarrow s', y \leftarrow t'$ | |
| | `return` $d, x, y$ | |

(c) Find $\gcd(128, 88)$:

| | | |
|---|---|---|
| Input: | $a \leftarrow$ ______, $b \leftarrow$ ______ | |
| Initialisation: | | |
| $r' \leftarrow 128, s' \leftarrow 1, t' \leftarrow 0,$ | $r' \leftarrow s' \times a + t' \times b = 1 \times 128 + 0 \times 88$ | = ______ |
| $r \leftarrow 88, s \leftarrow 0, t \leftarrow 1,$ | $r \leftarrow s \times a + t \times b = 0 \times 128 + 1 \times 88$ | = ______ |
| Iterations: | | |
| $q$ | $\leftarrow$ ______ | = ______ |
| $r$ | $\leftarrow$ ______ | = ______ |
| $s$ | $\leftarrow$ ______ | = ______ |
| $t$ | $\leftarrow$ ______ | = ______ |
| $s \cdot a + t \cdot b$ | = ______ | = ______ |
| | | |
| $q$ | $\leftarrow$ ______ | = ______ |
| $r$ | $\leftarrow$ ______ | = ______ |
| $s$ | $\leftarrow$ ______ | = ______ |
| $t$ | $\leftarrow$ ______ | = ______ |
| $s \cdot a + t \cdot b$ | = ______ | = ______ |
| | | |
| $q$ | $\leftarrow$ ______ | = ______ |
| $r$ | $\leftarrow$ ______ | = ______ |
| $s$ | $\leftarrow$ ______ | = ______ |
| $t$ | $\leftarrow$ ______ | = ______ |
| $s \cdot a + t \cdot b$ | = ______ | = ______ |
| Final: | $d \leftarrow r', x \leftarrow s', y \leftarrow t'$ | |
| | `return` $d, x, y$ | |

2. **Chinese Remainder Theorem**
Fill in the blanks.
The theorem states that given two equations as follows,

$$\begin{aligned} x &= a \pmod{M}, \text{ and} \\ x &= b \pmod{N} \end{aligned}$$

there is a unique solution $\pmod{M \cdot N}$ if and only if

$$\gcd(N, M) = 1.$$

The algorithm to find the solution is as follows:

| | | |
|---|---|---|
| Step 1: | Check if | $\gcd(M, N) = 1$ |
| Step 2: | Find | $T \leftarrow M^{-1} \pmod{N}$ |
| Step 3: | Find | $u \leftarrow (b - a) \cdot T \pmod{N}$ |
| Step 3: | Find | $x \leftarrow a + u \cdot M$ |

Note that $M^{-1} \pmod{N}$ can be found directly from the result of the extended Euclidean algorithm in the previous step.

(a) Consider the equations

$$\begin{aligned} x &= 6 \pmod{9}, \text{ and} \\ x &= 7 \pmod{25} \end{aligned}$$

The steps to follow according to CRT are

| | | |
|---|---|---|
| Step 1: | $\gcd(M, N)$ | $=$ ______ |
| Step 2: | So, | $T \leftarrow M^{-1} \pmod{N} = -11 =$ ______ |
| Step 3: | So, | $u \leftarrow (b - a) \cdot T \pmod{N} =$ ______ |
| Step 3: | So, | $x \leftarrow a + u \cdot M =$ ______ |

(b) Consider the equations

$$\begin{aligned} x &= 9 \pmod{100}, \text{ and} \\ x &= 20 \pmod{21} \end{aligned}$$

The steps to follow according to CRT are

| | | |
|---|---|---|
| Step 1: | $\gcd(M, N)$ | $=$ ______ |
| Step 2: | So, | $T \leftarrow M^{-1} \pmod{N} =$ ______ |
| Step 3: | So, | $u \leftarrow (b - a) \cdot T \pmod{N} =$ ______ |
| Step 3: | So, | $x \leftarrow a + u \cdot M =$ ______ |