UEE4611 Assignment #1 Solution

1. Find the mutiplicative inverse of each nonzero element in $\mathbb{Z}_7$.

$$\begin{aligned}
&\mathbb{Z}_7 \setminus \{0\} = \{1,2,3,4,5,6\} \\
&1 \times 1 \mod 7 = 1 \Rightarrow 1^{-1} = 1. \\
&2 \times 4 \mod 7 = 1 \Rightarrow 2^{-1} = 4. \\
&3 \times 5 \mod 7 = 1 \Rightarrow 3^{-1} = 5. \\
&4 \times 2 \mod 7 = 1 \Rightarrow 4^{-1} = 2. \\
&5 \times 3 \mod 7 = 1 \Rightarrow 5^{-1} = 3. \\
&6 \times 6 \mod 7 = 1 \Rightarrow 6^{-1} = 6.
\end{aligned}$$

2. The purpose of this problem is to set an upper bound on the number of iterations of the Euclidean algorithm.

(a) To prove $m/2 > r$, we can show that $m > 2r$. While $m = qn + r$, we need to show that $qn + r > 2r$.

$$\begin{aligned}
&qn + r > 2r \\
\Leftrightarrow\ &qn > r. \\
\because\ &q \geq 1 \,\&\, n > r \\
\Rightarrow\ &qn > r \\
\Rightarrow\ &m/2 > r.
\end{aligned}$$

(b)

$$\begin{aligned}
a &= qa_1 + a_2 \\
a_1 &= q_1 a_2 + a_3 \\
&\vdots \\
a_i &= q_i a_{i+1} + a_{i+2}
\end{aligned}$$

By (a), we can prove that $\frac{a_i}{2} > a_{i+2}$

(c) let $m > n$

$$
\begin{aligned}
& m = qn + r \\
\because\ & \frac{1}{2}a_i > a_{i+2}\,,\ \forall\, i \\
& \frac{1}{2}a_{i+2} > a_{i+4} \\
\Rightarrow & (\frac{1}{2})^2 a_i > a_{i+4} \\
\Rightarrow & (\frac{1}{2})^N a_i > a_{i+2N}
\end{aligned}
$$

While $m, n \le 2^N$, $(\frac{1}{2})^N \times m \le 1$, so $a_{i+2N} < 1$, and the only value it can be is 0.

And we know that the Euclidean algorithm terminates when the remainder is 0. So it will surely terminates after $2N$ steps.

3. Using the extended Euclidean algorithm, find the multiplicative inverse of

(a) $135 \mod 61$

$$\begin{aligned}
135 &= 2 \times 61 + 13 \\
61 &= 4 \times 13 + 9 \\
13 &= 1 \times 9 + 4 \\
9 &= 2 \times 4 + 1
\end{aligned}$$

$$\begin{aligned}
13 &= 135 - 2 \times 61 \\
9 &= 61 - 4 \times 13 \\
&= 61 - 4 \times (135 + 2 \times 61) \\
&= (-4) \times 135 + 9 \times 61
\end{aligned}$$

$$\begin{aligned}
4 &= 13 - 1 \times 9 \\
&= 135 - 2 \times 61 - (-4 \times 135 + 9 \times 61) \\
&= 5 \times 135 - 11 \times 61
\end{aligned}$$

$$\begin{aligned}
1 &= 9 - 2 \times 4 \\
&= (-4) \times 135 + 9 \times 61 - 2 \times (5 \times 135 - 11 \times 61) \\
&= (-14) \times 135 + 31 \times 61
\end{aligned}$$

$$\begin{aligned}
&(-14) \times 135 + 31 \times 61 \equiv 1(\mod 61) \\
\Rightarrow &(-14) \times 135 \equiv 1(\mod 61) \\
\Rightarrow &(-14) \times 135 + 61 \times 135 \equiv 1(\mod 61) \\
\Rightarrow &47 \times 135 \equiv 1(\mod 61)
\end{aligned}$$

The multiplicative inverse of $135 \mod 61$ is $47 \mod 61$.

(b) $7465 \mod 2464$

$$
\begin{aligned}
7465 &= 3 \times 2464 + 73 \\
2464 &= 33 \times 73 + 55 \\
73 &= 1 \times 55 + 18 \\
55 &= 3 \times 18 + 1
\end{aligned}
$$

$$
\begin{aligned}
73 &= 7465 - 3 \times 2464 \\
55 &= 2464 - 33 \times 73 \\
&= 2464 - 33 \times (7465 - 3 \times 2464) \\
&= 2464 - 33 \times 7465 + 99 \times 2464 \\
18 &= 73 - 1 \times 55 \\
&= 7465 - 3 \times 2464 + 33 \times 7465 - 100 \times 2464 \\
&= 34 \times 7465 - 103 \times 2464 \\
1 &= 55 - 3 \times 18 \\
&= 100 \times 2464 - 33 \times 7465 - 102 \times 7465 + 309 \times 2464 \\
&= 409 \times 2464 - 135 \times 7465
\end{aligned}
$$

$$
\begin{aligned}
& 409 \times 2464 - 135 \times 7465 \equiv 1 (\mod 2464) \\
\Rightarrow & (-135) \times 7465 \equiv 1 (\mod 2464) \\
\Rightarrow & (-135) \times 7465 + 2464 \times 7465 \equiv 1 (\mod 2464) \\
\Rightarrow & 2329 \times 7465 \equiv 1 (\mod 2464)
\end{aligned}
$$

The multiplicative inverse of $7465 \mod 2464$ is $2329 \mod 2464$.

4. Use Euler's theorem to find a number a between 0 and 92 with a congruent to 7^{1013} *modulo* 93.

$$\begin{aligned}
a^{\phi(n)} &\equiv 1 \pmod{n}, \quad \text{if} \gcd(a.n) = 1. \\
\phi(93) &= \phi(3) \times \phi(31) \\
&= 2 \times 30 \\
&= 60.
\end{aligned}$$

$$\begin{aligned}
7^{60} &\equiv 1 \pmod{93} \\
7^{1013} &\equiv 7^{60 \times 16} \times 7^{53} \pmod{93} \\
&= 7^{53} \pmod{93}
\end{aligned}$$

$$\begin{aligned}
7 &\equiv 7 \pmod{93} \\
7^2 &\equiv 49 \pmod{93} \\
7^4 &\equiv 76 \pmod{93} \\
7^8 &\equiv 10 \pmod{93} \\
7^{16} &\equiv 7 \pmod{93} \\
7^{15} &\equiv 1 \pmod{93}
\end{aligned}$$

$$\begin{aligned}
7^{53} &\equiv (7^{15})^3 \times 7^8 \pmod{93} \\
&\equiv 7^8 \pmod{93} \\
&\equiv 10 \pmod{93}
\end{aligned}$$

5. Use Euler's theorem to find a number a between 0 and 9 with a congruent to $9^{101}\, modulo\, 10$.

$$\begin{aligned} a^{\phi(n)} &\equiv 1(\mod n), \quad \text{if}\,\gcd(a.n)=1. \\ \phi(10) &= \phi(2)\times\phi(5) \\ &= 1\times 4 \\ &= 4. \end{aligned}$$

$$\therefore 9^4 \equiv\ 1(\mod 10).$$

$$\begin{aligned} \text{Thus, } 9^{101} &\equiv (9^4)^{25}\times 9(\mod 10) \\ &\equiv 9(\mod 10) \end{aligned}$$