MATH 240 Assignment 3

Mihail Anghelici 260928404

March 8, 2021

Question 1

(a)

$$28 = \{1, 2, 4, 7, 14\} \to \sum = 28 \checkmark$$
$$496 = \{1, 2, 4, 8, 16, 31, 62, 124, 248\} \to \sum = 496 \checkmark$$

(b)

The set of divisors of $2^{n-1}(2^n - 1)$ are

$$1, 2, \ldots, 2^{n-1}, 2^n - 1, 2(2^n - 1), \ldots 2^{n-1}(2^n - 1)$$
$$\implies S_n = (1 + (2^n - 1))(1 + 2 + \cdots + 2^{n-1})$$

Now since the second term is a closed-form geometric series we may use the geometric series formula

$$\sum_{k=1}^{n-1} ar^k = a\left(\frac{1 - r^n}{1 - r}\right) = \left(\frac{1 - 2^n}{1 - 2}\right) = 2^n - 1.$$

Thus, we have

$$S_n = 2^n(2^n - 1),$$

which is indeed equal to the initial expression divided by 2, i.e., the sum of its divisors other than itself. We conclude that the initial expression is perfect.

Question 2

(a)

$$\begin{aligned}
x_1 &= 15x_0 + 30 && \text{mod } 225\\
&= (15)(10) + 30 && \text{mod } 225\\
&= 180 && \text{mod } 225\\
&= 180\\
x_2 &= 15x_1 + 30 && \text{mod } 225\\
&= 15(180) + 30 && \text{mod } 225\\
&= 30\\
x_3 &= 15x_2 + 30 && \text{mod } 225\\
&= (15)(30) + 30 && \text{mod } 225\\
&= 30\\
&\vdots
\end{aligned}$$

Here we have a recursion, so we conclude the first 10 numbers are

$$\{180, 30, 30, 30, 30, 30, 30, 30, 30, 30\}.$$

(b)

$$\begin{aligned}
x_1 &= 13x_0 + 19 && \text{mod } 100 & x_6 &= 13x_5 + 19 && \text{mod } 100\\
&= 13(11) + 19 && \text{mod } 100 & &= 13(2) + 19 && \text{mod } 100\\
&= 162 && \text{mod } 100 & &= 45 && \text{mod } 100\\
&= 62 & & & &= 45\\
x_2 &= 13x_1 + 19 && \text{mod } 100 & x_7 &= 13x_6 + 19 && \text{mod } 100\\
&= 13(62) + 19 && \text{mod } 100 & &= 13(45) + 19 && \text{mod } 100\\
&= 825 && \text{mod } 100 & &= 604 && \text{mod } 100\\
&= 25 & & & &= 4\\
x_3 &= 13x_2 + 19 && \text{mod } 100 & x_8 &= 13x_7 + 19 && \text{mod } 100\\
&= 13(25) + 19 && \text{mod } 100 & &= 13(4) + 19 && \text{mod } 100\\
&= 344 && \text{mod } 100 & &= 71 && \text{mod } 100\\
&= 44 & & & &= 71\\
x_4 &= 13x_3 + 19 && \text{mod } 100 & x_9 &= 13x_8 + 19 && \text{mod } 100\\
&= 13(44) + 19 && \text{mod } 100 & &= 13(71) + 19 && \text{mod } 100\\
&= 591 && \text{mod } 100 & &= 942 && \text{mod } 100
\end{aligned}$$

$$\begin{aligned} &= 91 & & \qquad & &= 42 \\ x_5 &= 13x_4 + 19 & &\mod 100 \qquad & x_{10} &= 13x_9 + 19 & &\mod 100 \\ &= 13(91) + 19 & &\mod 100 \qquad & &= 13(42) + 19 & &\mod 100 \\ &= 1202 & &\mod 100 \qquad & &= 565 & &\mod 100 \\ &= 2 & & \qquad & &= 65 & & \end{aligned}$$

We conclude that the first 10 numbers are

$$\{62, 25, 44, 91, 2, 45, 4, 71, 42, 65\}.$$

Question 3

We need to first find the modular inverse for the congruence relationship $146s \equiv 1 \mod 421$. We use Euclid's algorithm then proceed by reversing.

$$\begin{aligned} 421 &= 2(146) + 129 \\ 146 &= 1(129) + 17 \\ 129 &= 7(17) + 10 \\ 17 &= 1(10) + 7 \\ 7 &= 2(3) + 1 \\ 3 &= 2(1) + 1 \\ 1 &= 1(1) + 0 \end{aligned} \qquad \Bigg| \qquad \begin{aligned} 1 &= 7 - (10 - 7) \\ &= 3(7) - 2(10) \\ &= 3(17 - 10) - 2(10) \\ &= 3(17) - 5(129 - 7(7)) \\ &= 38(146 - 129) - 5(129) \\ &= 38(146) - 43(421 - 146(2)) \\ &= 124(146) - 43(421) \end{aligned}$$

so we conclude that $146^{-1} = 124$, such that $146(146^{-1}) \equiv 1 \mod 421$. Finally,

$$146(146^{-1})x \equiv 12(124^{-1}) \Longrightarrow x = 225.$$

Question 4

(a)

First we note that $2407 = 126(19) + 13$ and $p - 1 = 18$, so

$$\begin{aligned} 2407^{1335} \mod 19 &\equiv 13^{1335} & &\mod 19 \\ &\equiv 13^{18(74)+3} & &\mod 19 \\ &\equiv \underbrace{(13^{18})^{74}}_{\equiv 1 \text{ FLT}} 13^3 & &\mod 19 \\ &\equiv 13^3 & &\mod 19 \\ &\equiv 2197 & &\mod 19 \end{aligned}$$

Since $2197 = 115(19) + 12$ then

$$\equiv 12$$

(b)

We use $p-1 = 348$, so

$$\begin{aligned} 7^{42806} \mod 349 &\equiv 7^{348(123)+2} && \mod 349 \\ &\equiv \underbrace{(7^{348})}_{\equiv 1 \text{ FLT}}{}^{123} 7^2 && \mod 349 \\ &\equiv 7^2 && \mod 349 \\ &\equiv 49 && \mod 349 \\ &\equiv 49 \end{aligned}$$

Question 5

(a)

$$11^{1329} \mod 1330 \equiv (11^3)^{443} \mod 1330$$

We note that $11^3 = 1331 = 1(1330) + 1$ so $1331 \equiv 1 \mod 1330$;

$$\begin{aligned} &\equiv 1^{443} \mod 1330 \\ &\equiv 1 \mod 1330 \ \checkmark \end{aligned}$$

The test is passed.

(b)

No it is a false positive, indeed, by theorem, n prime $\iff \forall 0 < a < n-1\ , a^{n-1} \equiv 1 \mod n$. Here, n is not prime since it is divisible by 2 , so $a^{n-1} \equiv 1 \mod n$ from part (a) must be false as well.

Question 6

(a)

$$\begin{aligned} \hat{M} &= M^p && \mod n \\ &= 9^7 && \mod 209 \\ &= (9^3)^2 9 && \mod 209 \\ &= 102^2 9 && \mod 209 \\ &= (10404)9 && \mod 209 \end{aligned}$$

Since $10404 = 209(49) + 163 = 163 \mod 209$,

$$= (163)9 \qquad \mod 209$$

$$= 1467 \qquad \mod 209$$
$$= 4$$

We conclude that $\hat{M} = 9^7 \mod 209 = 4$.

(b)

We look for p^{-1} in $7p^{-1} \equiv 1 \mod 180$, where $180 = (q_1 - 1)(q_2 - 1)$. We use Euclid's algorithm and reverse;

$$\begin{aligned} 180 &= 25(7) + 5 \\ 7 &= 1(5) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2) + 0 \end{aligned} \qquad \Bigg| \qquad \begin{aligned} 1 &= 5 - 2(7 - 5) \\ &= 3(5) - 2(7) \\ &= 3(180 - 25(7)) - 2(7) \\ &= 3(180) - 77(7) \end{aligned}$$

So we have that $p^{-1} = -77$. We can add 180 to this number and the congruence relationship is kept so we conclude $p^{-1} = x = 103$.

(c)

$$M = \hat{M}^x \mod n = 4^{103} \mod 209 = 9.$$

Remark. *I was not able to simplify the latter expression, indeed* $\nexists\ s \leq 20 \in \mathbb{N} \mid 4^s \mod 209 = 1 \vee 2$*, the answer was computed numerically.*