Mathematics Homework Sheet 4

Authors: Abdullah Oguz Topcuoglu & Ahmed Waleed Ahmed Badawy Shora

Problem 1

Question is asking to find Bezout coefficients.

$$\begin{aligned}
1552303 &= 6 \cdot 233927 + 148741, & u_2 &= u_0 - 6u_1 = 1, & v_2 &= v_0 - 6v_1 = -6\\
233927 &= 1 \cdot 148741 + 85186, & u_3 &= u_1 - u_2 = -1, & v_3 &= v_1 - v_2 = 7\\
148741 &= 1 \cdot 85186 + 63555, & u_4 &= u_2 - u_3 = 2, & v_4 &= v_2 - v_3 = -13\\
85186 &= 1 \cdot 63555 + 21631, & u_5 &= u_3 - u_4 = -3, & v_5 &= v_3 - v_4 = 20\\
63555 &= 2 \cdot 21631 + 20293, & u_6 &= u_4 - 2u_5 = 8, & v_6 &= v_4 - 2v_5 = -53\\
21631 &= 1 \cdot 20293 + 1338, & u_7 &= u_5 - u_6 = -11, & v_7 &= v_5 - v_6 = 73\\
20293 &= 15 \cdot 1338 + 223, & u_8 &= u_6 - 15u_7 = 173, & v_8 &= v_6 - 15v_7 = -1148\\
1338 &= 6 \cdot 223 + 0,
\end{aligned}$$

Which means that $(1552303, 233927) = 223$. And we have the Bezout coefficients $u_8 = 173, v_8 = -1148$

$$1552303 \cdot 173 + 233927 \cdot (-1148) = 223$$

Thus $m = 173, n = -1148$.

Problem 2

Start with the fact that $106 \equiv 106 \mod 143$.

$$\begin{aligned}
106 &\equiv 106 \mod 143 && \text{(Square both sides)}\\
106^2 = 11236 &\equiv 82 \mod 143 && \text{(Square both sides)}\\
106^4 &\equiv 82^2 \equiv 3 \mod 143 && \text{(Square both sides)}\\
106^8 &\equiv 3^2 \equiv 9 \mod 143
\end{aligned}$$

And note these:

$$\begin{aligned}
106^2 &= 11236 = 78 \cdot 143 + 82\\
82^2 &= 6724 = 46 \cdot 143 + 3\\
3^2 &= 9 = 0 \cdot 143 + 9
\end{aligned}$$

Now we can compute 106^{11}:

$$\begin{aligned}
106^{11} &= 106^8 \cdot 106^2 \cdot 106 \\
&\equiv 9 \cdot 82 \cdot 106 \mod 143 \\
&\equiv 738 \cdot 106 \mod 143 \\
&\equiv (5 \cdot 143 + 23) \cdot 106 \mod 143 \\
&\equiv 23 \cdot 106 \mod 143 \\
&\equiv 2428 \mod 143 \\
&\equiv (16 \cdot 143 + 140) \mod 143 \\
&\equiv 140 \mod 143
\end{aligned}$$

So, these are the results:

$$\begin{gathered}
106^2 \equiv 82 \mod 143 \\
106^4 \equiv 3 \mod 143 \\
106^8 \equiv 9 \mod 143 \\
106^{11} \equiv 140 \mod 143
\end{gathered}$$

Problem 3

(a)

We have the system of equations:

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 5 \mod 7 \\ x \equiv 8 \mod 11 \end{cases}$$

Let's first solve the first two equations:

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 5 \mod 7 \end{cases}$$

From chinese remainder theorem we know that $x = 14m + 15n$ where m and n are Bezout coefficients of 3 and 7. We can find them using the extended Euclidean algorithm:

$$\begin{aligned}
&7 = 2 \cdot 3 + 1, \qquad && u_2 = u_0 - 2u_1 = 1, \quad v_2 = v_0 - 2v_1 = -2 \\
&3 = 3 \cdot 1 + 0
\end{aligned}$$

$$\begin{aligned}
m &= u_2 = 1 \\
n &= v_2 = -2 \\
x &= 14m + 15n \\
x &= 14 \cdot 1 + 15 \cdot (-2) \\
x &= 14 - 30 \\
x &= -16 \mod 21 \\
x &= 5 \mod 21
\end{aligned}$$

Now we have these two equations:

$$\begin{cases} x \equiv 5 \mod 21 \\ x \equiv 8 \mod 11 \end{cases}$$

We can solve this system of equations using the same method:

$$\begin{aligned}
&21 = 1 \cdot 11 + 10, && u_2 = u_0 - u_1 = 1, \quad v_2 = v_0 - v_1 = -1 \\
&11 = 1 \cdot 10 + 1, && u_3 = u_1 - u_2 = -1, \quad v_3 = v_1 - v_2 = 2 \\
&10 = 10 \cdot 1 + 0
\end{aligned}$$

$$\begin{aligned}
m &= u_3 = -1 \\
n &= v_3 = 2 \\
x &= 168m + 55n \\
x &= 168 \cdot (-1) + 55 \cdot 2 \\
x &= -168 + 110 \\
x &= -58 \mod 231 \\
x &= 173 \mod 231
\end{aligned}$$

Problem 4

(a)

Fermat's little theorem states that if p is a prime number and a is an integer not divisible by p, then:

$$a^{p-1} \equiv 1 \mod p$$

63 is not a prime number:

We are gonna try to prove this by showing a contradiction. Let's take $a = 2$ and $p = 63$. Then according to Fermat's little theorem we have:

$$2^{62} \equiv 1 \mod 63$$

We are given the hint that $2^6 \equiv 1 \mod 63$.

$$\begin{aligned} 2^{62} = (2^6)^{10} \cdot 2^2 &\equiv 2^2 \mod 63 \\ &\equiv 4 \mod 63 \end{aligned}$$

This result contradicts the Fermat's little theorem, which proves that 63 is not a prime number.
341 is not a prime number:
We are gonna try to prove this by showing a contradiction. Let's take $a = 56$ and $p = 341$. Then according to Fermat's little theorem we have:

$$56^{340} \equiv 1 \mod 341$$

We are given the hint that $56^3 \equiv 1 \mod 341$.

$$\begin{aligned} 56^{340} = (56^3)^{113} \cdot 56^1 &\equiv 56^1 \mod 341 \\ &\equiv 56 \mod 341 \end{aligned}$$

This result contradicts the Fermat's little theorem, which proves that 341 is not a prime number.

(c)

We want to show that:

$$(a+b)^p \equiv a^p + b^p \mod p$$

Fermat's little theorem says that

$$a^{p-1} \equiv 1 \mod p \qquad if \quad (a, p) = 1$$

Multiplying both sides by a we get:

$$a^p \equiv a \mod p \qquad (1)$$

We have the same thing for b too:

$$b^p \equiv b \mod p \qquad (2)$$

And we have the same thing for $a + b$:

$$(a+b)^p \equiv a + b \mod p$$

Adding equations (1) and (2) we get:

$$a^p + b^p \equiv a + b \mod p$$

Which happens to be equal to $(a+b)^p$ in mod p. Thus we have shown that:

$$(a+b)^p \equiv a^p + b^p \equiv a + b \mod p$$