CSCI 2824 – Fall 2021

Homework 6

Name: XXXXXXX XXXXXXX Student ID: ZZZZZZZZZ

This assignment is due on Friday, October 15th to Gradescope by 6PM. There are 5 questions on this homework. You are expected to write or type up your solutions neatly. Remember that you are encouraged to discuss problems with your classmates, but you must work and write your solutions on your own.

Important: Make sure to clearly write your full name and your student ID number at the top of your assignment. You may **neatly** type your solutions in LaTeX for extra credit on the assignment. Make sure that your images/scans are clear or you will lose points/possibly be given a 0. Additionally, please be sure to match the problems from the Gradescope outline to your uploaded images.

1. Convert each of the following to their respective Decimal, Octal, Hexadecimal and binary representation:

   (a) $(742)_8$

   (b) $(1011)_2$

   (c) $(47)_{10}$

   (d) $(3EAC)_{16}$

   Solution: (a) $(742)_8$
   Decimal: 482
   Hex: 1E2
   Binary: 111100010

   (b) $(1011)_2$
   Decimal: 11
   Hex : B
   Octal: 13

   (c) $(47)_{10}$
   Binary: 101111
   Hex: 2 F
   Octal: 57

   (d) $(3EAC)_{16}$
   Decimal: 16044
   Binary: 11111010101100
   Octal: 37254

2. Let a and b be two Natural Numbers, such that the greatest common divisor of a and b is 63, and the least common multiple of a and b is 44452800. If 'b' is an odd number, what is the minimum value of 'a' possible? [Hint: a · b = gcd(a, b) · lcm(a, b)]

   Solution:

   Since, a · b = gcd(a, b) · lcm(a, b)

   and
   By prime factorization, 63 can also be expressed as: $3^2 \times 7$
   By prime factorization, 44452800 can also be expressed as: $2^6 \times 3^4 \times 5^2 \times 7^3$

   So finally we have:
   a · b = $(3^2 \times 7) \cdot (2^6 \times 3^4 \times 5^2 \times 7^3) = 2^6 \times 3^6 \times 5^2 \times 7^4$

   What we can conclude about a:
   1. Given that b is an odd number, the 2^6 in the $a \cdot b$ given above must be a factor of a and not a factor of b.
   2. Since gcd(a,b) = 63, $63|a$ (By definition of gcd). Therefore, 63 must also be a factor of a.

   Considering both the conclusions above, the minimum value of a has to be $2^6 \times 63 = 64 \times 63 = 4032$. Finally, a=4032.

3. Find out if the following numbers are prime numbers, show your work:

   (a) 773

   (b) 733

   (c) 377

   Solution:

   (a) Prime numbers smaller than $\sqrt{773}$: $\sqrt{773} > [2, 3, 5, 7, 11, 13, 17, 19, 23]$

   $773 \bmod 2 = 1$ Not a divisor.
   $773 \bmod 3 = 2$ Not a divisor.
   $773 \bmod 5 = 3$ Not a divisor.
   $773 \bmod 7 = 3$ Not a divisor.
   $773 \bmod 11 = 3$ Not a divisor.
   $773 \bmod 13 = 6$ Not a divisor.
   $773 \bmod 17 = 8$ Not a divisor.
   $773 \bmod 19 = 9$ Not a divisor.
   $773 \bmod 23 = 14$ Not a divisor.

   No prime number less than $\sqrt{773}$ is a factor. So, 773 is a prime number!

   (b) Prime numbers smaller than $\sqrt{733}$: $\sqrt{733} > [2, 3, 5, 7, 11, 13, 17, 19, 23]$

   $733 \bmod 2 = 1$ Not a divisor.
   $733 \bmod 3 = 1$ Not a divisor.
   $733 \bmod 5 = 3$ Not a divisor.
   $733 \bmod 7 = 5$ Not a divisor.
   $733 \bmod 11 = 7$ Not a divisor.
   $733 \bmod 13 = 5$ Not a divisor.
   $733 \bmod 17 = 2$ Not a divisor.
   $733 \bmod 19 = 11$ Not a divisor.
   $733 \bmod 23 = 20$ Not a divisor.

   No prime number less than $\sqrt{773}$ is a factor. So, 773 is a prime number!

   (c) Prime numbers smaller than $\sqrt{377}$: $\sqrt{377} > [2, 3, 5, 7, 11, 13, 17, 19]$

   $377 \bmod 2 = 1$ Not a divisor.
   $377 \bmod 3 = 2$ Not a divisor.
   $377 \bmod 5 = 2$ Not a divisor.
   $377 \bmod 7 = 6$ Not a divisor.
   $377 \bmod 11 = 3$ Not a divisor.
   $377 \bmod 13 = 0$ $\rightarrow$ divisor.

   We don't need to check for 17 since we already found a factor. Since 377 has 13 as a factor, it is not a prime number!

4. Find out of the inverse exists for the following, give reasoning behind your answer. If you conclude that the inverse exists then find the Bézout coefficients and the inverse of the modulo. [Hint: Example 2 of section 4.4 in the book]

   (a) 678 modulo 2970

   (b) 137 modulo 2350

   Solution:

   (a) For an inverse to exist, 2970 and 678 must be co-primes or relatively primes and 678 must be greater than 1 (which it is).
   using euclidean algorithm:

$$
\begin{aligned}
2970 &= 678 \times 4 + 258 \\
678 &= 258 \times 2 + 162 \\
258 &= 162 \times 1 + 96 \\
162 &= 96 \times 1 + 66 \\
96 &= 66 \times 1 + 30 \\
66 &= 30 \times 2 + 6 \\
30 &= 6 \times 5 + 0
\end{aligned}
$$

This means that the $gcd(2970, 678) = 6$ so 2970 and 678 are not co-primes. So the inverse does not exist.

(b) For an inverse to exist, 2350 and 137 must be co-primes or relatively primes and 137 must be greater than 1 (which it is).

using euclidean algorithm:

$$
\begin{aligned}
2350 &= 137 \times 17 + 21 \\
137 &= 21 \times 6 + 11 \\
21 &= 11 \times 1 + 10 \\
11 &= 10 \times 1 + \mathbf{1}
\end{aligned}
$$

Meaning, 2350 and 137 are relatively prime, so the inverse exists. We can now find the Bézout coefficients by working the euclidean algorithm backwards:

$$
\begin{aligned}
1 &= 11 - 1 \cdot 10 \\
&= 11 - 1 \cdot (21 - 11) = 11 - 1 \cdot 21 + 11 = -1 \cdot 21 + 2 \cdot 11 \\
&= -1 \cdot 21 - 2 \cdot (137 - 21 \times 6) = -1 \cdot 21 + 2 \cdot 137 - 2 \cdot 21 \cdot 6 \\
&= -1 \cdot 21 - 12 \cdot 21 + 2 \cdot 137 = -13 \cdot 21 + 2 \cdot 137 \\
&= -13 \cdot (2350 - 137 \cdot 17) + 2 \cdot 137 = -13 \cdot 2350 + 13 \cdot 137 \cdot 17 + 2 \cdot 137 \\
&= -13 \cdot 2350 + (13 \times 17 + 2) \cdot 137 = -13 \cdot 2350 + 223 \cdot 137 \\
&= -30550 + 30551 = 1
\end{aligned}
$$

Now, from the above we can conclude that the Bézout coefficients are: -13 and 223. This makes the inverse as 223.

5. Solve the following:

   (a) $123^{1001} (\text{mod } 101)$

   (b) $17^{123} (\text{mod } 13)$

Solution:

(a) $123^{1001} (\text{mod } 101)$

Since 101 is a prime number and 123 is not divisible by 101, we can apply Fermat's little theorem to this. Using Fermat's little theorem we can say: $123^{100} \text{ mod } 101 \equiv 1 \text{ mod } 101$.

1001 can be expressed as: $1000 + 1 = 100 \times 10 + 1$

$$
123^{1001} (\text{mod } 101) = 123^{100 \times 10 + 1} (\text{mod } 101) = (123^{100})^{10} \cdot 123^{1} (\text{mod } 101)
$$

Since $(a \cdot b) \bmod m \equiv ((a \bmod m) \cdot (b \bmod m)) \bmod m$

$$\begin{aligned}((123^{100})^{10} \cdot 123^1) \bmod 101 &= ((123^{100})^{10} \bmod 101 \cdot 123^1 \bmod 101) \bmod 101 \\ &= ((123^{100} \bmod 101)^{10} \bmod 101 \cdot 22) \bmod 101 \\ &= (1^{10} \bmod 101 \cdot 22) \bmod 101 \\ &= (1 \bmod 101 \cdot 22) \bmod 101 \\ &= (1 \cdot 22) \bmod 101 \\ &= (22) \bmod 101 = 22\end{aligned}$$

Therefore, $123^{1001} (\text{mod } 101) = 22$.

(b) $17^{123} (\text{mod } 13)$

Since 13 is a prime number and 17 is not divisible by 13, we can apply Fermat's little theorem to this. Using Fermat's little theorem we can say: $17^{12} \bmod 13 \equiv 1 \bmod 13$.

123 can be expressed as: $120 + 3 = 12 \times 10 + 3$

$$17^{123} (\text{mod } 13) = 17^{12 \times 10 + 3} (\text{mod } 13) = (17^{12})^{10} \cdot 17^3 (\text{mod } 13)$$

Since $(a \cdot b) \bmod m \equiv ((a \bmod m) \cdot (b \bmod m)) \bmod m$

$$\begin{aligned}((17^{12})^{10} \cdot 17^3) \bmod 13 &= ((17^{12})^{10} \bmod 13 \cdot 17^3 \bmod 13) \bmod 13 \\ &= [(17^{12} \bmod 13)^{10} \bmod 13 \cdot (17 \bmod 13)^3 \bmod 13] \bmod 13 \\ &= [(1 \bmod 13)^{10} \bmod 13 \cdot (4)^3 \bmod 13] \bmod 13 \\ &= [(1)^{10} \bmod 13 \cdot 64 \bmod 13] \bmod 13 \\ &= [1 \bmod 13 \cdot 12] \bmod 13 \\ &= [1 \cdot 12] \bmod 13 \\ &= [12] \bmod 13 = 12\end{aligned}$$

Therefore, $17^{123} (\text{mod } 13) = 12$.