Assignment #8, CSE 191

Fall, 2014

Solution

General Guidelines:

This assignment will NOT be collected, nor graded. However, you should carefully complete it as if it were to be graded. There will be a quiz based on this assignment (with very similar problems) during the week Nov 10 - 14.

The solution will be posted on Monday, Nov 10.

1. (0 points). Page 272, Problem 5.

Solution: $10! = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

2. (0 points). Page 272, Problem 6.

Sol: Let $N = 100!$. For each 0 at the end of N, we need a factor 5 and a factor 2. It is clear that the number of factors 2 in N is far more than the number of factors 5 in N. So it is enough to count the number of factors 5 in N.

Each of the numbers: $\{5, 10, 15, \ldots, 95, 100\}$ contributes one factor 5 to N.

In addition, each of $\{25, 50, 75, 100\}$ contributes one additional factor 5 to N.

Thus there are a total of 24 factors 5 in N. So there are 24 0's at the end of N.

3. (0 points). Page 272, Problem 14.

Solution: $1, 5, 7, 11$.

4. (0 points). Page 272, Problem 17 (b) (c) (d).

Sol: (b): 14, 15, 21: No, because $gcd(14, 21) = 7 \neq 1$.
(c) 12, 17, 31, 37. Yes
(d) 17, 18, 19, 23. Yes.

5. (0 point). Page 273, Problem 25 and 26 (a) (b) (c) (d) (e)

Solution: (a) $a = 3^7 \cdot 5^3 \cdot 7^3$ and $b = 2^{11} \cdot 3^5 \cdot 5^9$.
$gcd(a, b) = 3^5 \cdot 5^3$ and $lcm(a, b) = 2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$.

(b) $a = 11 \cdot 13 \cdot 17$ and $b = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$.
$gcd(a, b) = 1$ and $lcm(a, b) = a \cdot b = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$.

(c) $a = 23^{31}$ and $b = 23^{17}$.
$gcd(a, b) = 23^{17}$ and $lcm(a, b) = 23^{31}$.

(d) $a = 41 \cdot 43 \cdot 53$ and $b = 41 \cdot 43 \cdot 53$.
$gcd(a, b) = lcm(a, b) = 41 \cdot 43 \cdot 53$.

(e) $a = 3^{13} \cdot 5^{17}$ and $b = 2^{12} \cdot 7^{21}$.
$gcd(a, b) = 1$ and $lcm(a, b) = a \cdot b = 2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$.

6. (0 point). Page 273, Problem 30. (It is good enough to express the lcm as the product of its prime factors.)

Sol: For any two integers a and b, we have $gcd(a,b) \cdot lcm(a,b) = a \cdot b$.
So $lcm(a,b) = a \cdot b / gcd(a,b) = 2^7 3^8 5^2 7^{11} / 2^3 3^4 5 = 2^4 \times 3^4 \times 5 \times 7^{11}$.

7. (0 points) Find the binary representation of 567.

Sol:

$$\begin{aligned}
571 &= 285 \cdot 2 + 1 \\
285 &= 142 \cdot 2 + 1 \\
142 &= 71 \cdot 2 + 0 \\
71 &= 35 \cdot 2 + 1 \\
35 &= 17 \cdot 2 + 1 \\
17 &= 8 \cdot 2 + 1 \\
8 &= 4 \cdot 2 + 0 \\
4 &= 2 \cdot 2 + 0 \\
2 &= 1 \cdot 2 + 0 \\
1 &= 0 \cdot 2 + 1
\end{aligned}$$

So: $571 = (1000111011)_2$
Check: $2^9 + 2^5 + 2^4 + 2^3 + 2^1 + 2^0 = 512 + 32 + 16 + 8 + 2 + 1 = 571$.

8. (0 points). This problem illustrates an example of the of RSA public key encryption process.
Pick $p = 103$ and $q = 211$. Then $n = p \cdot q = 103 \cdot 211 = 21733$. Also pick $e = 19$.
Thus $(n, e) = (21733, 19)$ is the public key.

1. We have $(p-1) \cdot (q-1) = 102 \cdot 210 = 21420$.

   Use Euclidean-GCD algorithm to show: $gcd(21420, 19) = 1$

   (You need to write down all intermediate steps. They are needed in the next part.)

2. Find integers d, t such that:

$$d \cdot e + t \cdot 21420 = d \cdot 19 + t \cdot 21420 = 1 \tag{1}$$

   This can be done by using Extended Euclidean-GCD algorithm. Namely, by reversing the process in part 1.

   Note that from (1), we have:

$$d \cdot e \equiv 1 \bmod 21420$$

   So $(n, d) = (21733, d)$ is the secrete key.

3. Suppose that Alice has a message $M = 100$. Calculate the encrypted message C, where:

$$C = M^e \bmod n = 100^{19} \bmod 21733$$

Note: You should NOT evaluate $M^2 \equiv \bmod 21733$, $M^3 \equiv \bmod 21733$, $M^4 \equiv \bmod 21733$, $\ldots, M^{19} \equiv \bmod 21733$. This will take too long! Instead, you should use the *double squaring* method discussed in class.

(The answer should be: $100^{19} \bmod 21733 = 20815$. You should find the solution by yourself. The answer is provided here so that you can proceed to the next step.)

4. Once Bob receives the encrypted message C, he needs to decrypt it by calculating:

$$C^d \equiv \bmod n$$

Perform this calculation (as in part 3, or write a short program to do this). Verify that this gives the original message $M = 100$.

This is a long process involving lengthy numerical calculations. You are encouraged to complete the entire calculation, and see the answer is indeed 100. If you don't have enough time, it is acceptable that you carry out the first few steps (so that you can understand what's going on), and wait to see the solution.

Sol:

1:

$$\begin{aligned} 21420 &= 1127 \times 19 + 7 \\ 19 &= 2 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \end{aligned}$$

2:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (7 - 5) \\ &= 5 - 2 \times 7 + 2 \times 5 \\ &= 3 \times 5 - 2 \times 7 \\ &= 3 \times (19 - 2 \times 7) - 2 \times 7 \\ &= 3 \times 19 - 6 \times 7 - 2 \times 7 \\ &= 3 \times 19 - 8 \times 7 \\ &= 3 \times 19 - 8 \times (21420 - 1127 \times 19) \\ &= (3 + 8 \times 1127) \times 19 - 8 \times 21420 \\ &= 9019 \times 19 - 8 \times 21420 \end{aligned}$$

3:

$$
\begin{aligned}
100 &\mod 21733 = 100 \\
100^2 &\mod 21733 = 10000 \\
100^4 &\mod 21733 = 6467 \\
100^8 &\mod 21733 = 6467^2 \mod 21733 = 7797 \\
100^{16} &\mod 21733 = 7797^2 \mod 21733 = 6008 \\
100^{19} &\mod 21733 = 100^{16} \times 100^2 \times 100 \mod 21733 = 6008 \times 100^2 \times 100 \mod 21733 = 20815
\end{aligned}
$$

In the last step, you calculate the product of 3 numbers from left to right. After calculating the product of the first two numbers (mod 21733), use the result to multiply the 3rd number (mod 21733).

4:

$$
\begin{aligned}
20815 &\mod 21733 = 20815 \\
20815^2 &\mod 21733 = 16870 \\
20815^4 &\mod 21733 = 16870^2 \mod 21733 = 3265 \\
20815^8 &\mod 21733 = 3265^2 \mod 21733 = 11055 \\
20815^{16} &\mod 21733 = 11055^2 \mod 21733 = 8366 \\
20815^{32} &\mod 21733 = 8366^2 \mod 21733 = 9696 \\
20815^{64} &\mod 21733 = 9696^2 \mod 21733 = 17191 \\
20815^{128} &\mod 21733 = 17191^2 \mod 21733 = 5147 \\
20815^{256} &\mod 21733 = 5147^2 \mod 21733 = 20815 \\
20815^{512} &\mod 21733 = 20815^2 \mod 21733 = 16870 \\
20815^{1024} &\mod 21733 = 16870^2 \mod 21733 = 3265 \\
20815^{2048} &\mod 21733 = 3265^2 \mod 21733 = 11055 \\
20815^{4096} &\mod 21733 = 11055^2 \mod 21733 = 8366 \\
20815^{8192} &\mod 21733 = 8366^2 \mod 21733 = 9696
\end{aligned}
$$

Note that: 9019 = 8192+512+256+32+16+8+2+1. So

$$
\begin{aligned}
20815^{9019} \mod 21733 =& 20815^{8192} \times 20815^{512} \times 20815^{256} \times 20815^{32} \times \\
& 20815^{16} \times 20815^{8} \times 20815^{2} \times 20815^{1} \mod 21733 \\
=& 9696 \times 16870 \times 20815 \times 9696 \times 8366 \times 11055 \times 16870 \times 20815 \mod 21733 \\
=& 100
\end{aligned}
$$

In the last step, you calculate the product of 8 numbers from left to right. After calculating the product of the first two numbers (mod 21733), use the result to multiply the 3rd number (mod 21733) ..... Continue this way until the entire product is calculated. (In this way, all numbers calculated in the intermediate steps are less than 21733).