CS/MATH111 ASSIGNMENT 2

Itzel Gonzalez SID: 861304050 and Jiunn Siow SID:861196669

April 2019

Problem 1: Let $n = p_1p_2...p_k$, where $p_1, p_2, ..., p_k$ are different primes. Prove that n has exactly 2^k different divisors. For example, if $n = 105$, then n $= 3 \cdot 5 \cdot 7$, so $k = 3$, and thus n has $2^3 = 8$ divisors. These divisors are: $1, 3, 5, 7, 15, 21, 35, 105$. Hint. You can reduce the problem to counting other objects that we already know how to count. Alternatively, this can be proved by induction on k.

Solution 1: We will be using Induction to prove this problem
Base case:
Assume that k = 1. As a result, we should get 2 divisors if we have one prime p_1.
Assume that n is any prime number. As a result we know that the two divisors are 1 and n itself
Therefore, the base case holds
Inductive Step:
We want to prove that for $n = p_1p_2...p_k$,that there are different prime numbers that there are 2^k different divisors
Assumption: We know that for $n = p_1p_2...p_{k-1}$ that there k-1 different primes and there are 2^{k-1} different divisors.

$n_1 = p_1p_2...p_{k-1}$	Following our assumption with a certain number n_1
$n_2 = n_1 \cdot p_k$	Multiply every prime number in n_1 by p_k to get a new divisor for each old divisor
$d_1 \cdot p^k = d_2$	d_1 is the set of all divisors from $n_1.d_2$ is the new set of divisors d_1 multiplied by p_k
$...d_{1_{k-1}} \cdot p^k = ...d_{2_{k-1}}$	

We need to add all the old and new divisors together. We know for both n_1 and n_2, that there are 2^{k-1} divisors

$2^k = d_1 + d_2$	Following from before
$2^k = 2^{k-1} + 2^{k-1}$	Counting current primes and new primes
$2^k = \frac{1}{2} \cdot 2^k + \frac{1}{2} \cdot 2^{k-1}$	

Therefore, by induction we know that for $n = p_1p_2...p_k$ that there are 2^k divisors.
We accounted for all the divisors that either contained p_k or did not contain p_k.
d_1 contained all the divisors that did not contain p_k and d_2 accounted for divisors that contained p_k

---

Problem 2: Alice's RSA public key is $P = (e, n) = (13, 77)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 2, B is 3, ..., Z is 27, and blank is 28. Then he uses RSA to encode each number separately.

Bob's encoded message is:

10	7	58	30	23	62
7	64	62	23	62	61
7	41	62	21	7	49
75	7	69	53	58	37
37	41	10	64	50	7
10	64	21	62	61	35
62	61	62	7	52	10
21	58	7	49	75	7
62	26	22	53	30	21

`10 37 64`

Decode Bob's message. Notice that you don't have Bob's secrete key, so you need to "break" RSA to decrypt his message.

For the solution, you need to provide the following:

- Describe step by step how you arrived at the solution. In particular, explain how you determined p, q, $\phi(n)$, and d.
- Show the calculation that determines the first letter in the message from the first number in ciphertext.
- Give Bob's message in plaintext. The message is a quote. Who said it?
- If you wrote a program, attach your code to the hard copy. If you solved it by hand (not recommended), attach your scratch paper with calculations for at least 5 first letters.

Suggestion: this can be solved by hand, but it will probably be faster to write a short program.

Solution 2:

- Describe steps of solution:
  We find p and q from n, we are given n = 77.
  The only prime factors of 77 are 7 and 11.
  So, p = 7 and q = 11.

  Next, we find totient function $\phi(n)$.
  $\phi(77) = (p-1)(q-1) = 6 * 10 = 60$

  Next, we solve for d using formula: $d = e^{-1} mod(\phi(n))$
  Plugging in $e = 13$ and $\phi(n) = 60$: $d = 13^{-1} mod(60)$
  Since 60 is not prime, we cannot use Fermat's Little Theorem

  But we can use Euclid's Algorithm: $gcd(60, 13)$
  $60 = 13(4) + 8 \rightarrow 8 = 60 - 13(4)$
  $13 = 8(1) + 5 \rightarrow 5 = 13 - 8$
  $8 = 5(1) + 3 \rightarrow 3 = 8 - 5$
  $5 = 3(1) + 2 \rightarrow 2 = 5 - 3$
  $3 = 2(1) + 1 \rightarrow 1 = 3 - 2$

  $1 = 3 - [5 - 3] \rightarrow 1 = 2(3) - 5$
  $1 = 2[8 - 5] - 5 \rightarrow 1 = 2(8) - 3(5)$
  $1 = 2[8 - 5] - 5 \rightarrow 1 = 5(8) - 3(13)$
  $1 = 5[60 - 4(13)] - 3(13) \rightarrow 1 = 5(60) - 20(13) - 3(13)$
  $1 = 5(60) - 23(13)$
  $d = -23 mod(60) \rightarrow d = 37$

  Next, we decrypt message using formula: $M = C^d mod(n)$
  Our formula is: $M = C^{37} mod(77)$

- We can decrypt the letter for the first number in the ciphertext using C = 10.
  $M = C^{37} mod(77) \rightarrow M = 10^{37} mod(77)$

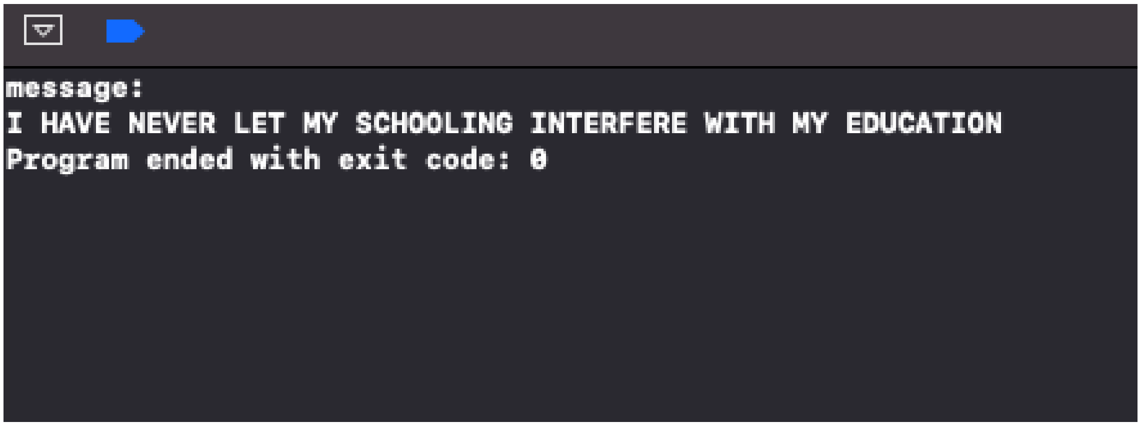
$M = (10^2)^{18} * 10 mod(77)$
$10^2 mod(77) = 23$
$10^4 mod(77) = (10^2)^2 mod(77) = (23)^2 mod(77) = 67$
$10^8 mod(77) = (10^4)^2 mod(77) = (67)^2 mod(77) = 23$
$10^{16} mod(77) = (10^8)^2 mod(77) = (23)^2 mod(77) = 67$
$10^{32} mod(77) = (10^{16})^2 mod(77) = (67)^2 mod(77) = 23$
$10^{37} mod(77) = (10^{32} * 10^4 * 10) mod(77) = (23 * 67 * 10) mod(77) = 10$
$M = 10$

- Give Bob's message in plaintext. The message is a quote. Who said it?
  "I HAVE NEVER LET MY SCHOOLING INTERFERE WITH MY EDUCATION" by Mark Twain

Code for RSA Decryption:

```
RSA 〉 My Mac                                   Finish
RSA 〉 RSA 〉 main.cpp 〉 decrypt(vector<int> message, int n, int d)

//  main.cpp
//  RSA
//
//  Created by Itzel G on 4/30/19.
//  Copyright © 2019 Itzel G. All rights reserved.
#include <iostream>
#include <sstream>
#include <vector>
#include <cmath>

using namespace std;

//find prime numbers p1 & p2 given n
int breakRSA();
void decrypt(vector<int> message, int n, int d);

int main(int argc, const char * argv[]) {
    //Given:
    //   Public key: e= 13 n = 77
    //   and message (each letter: C)

    //1. Find prime numbers.
    //   p = 7, q = 11

    //2. Find phi_n = (p - 1)(q - 1).
    //   phi_n = 60

    //3. Solve for d.
    //   d = (1/e)%phi_n
    //   d = (1/13)%60 = 37
    //   Euclid's Algorithm: d = gcd(e, n)

    //4. Decrypt function does:
    //   M = C^d mod(n)  -> M = C^37mod(77) (written)
    //   M = pow(C, d)%n -> M = pow(C, 37)%77 (c++ code)
    //   * prints M as char

    int e = 13, n = 77;
    int phi_n = 60;
    int d = 37;
```

```cpp

    vector<int> message =
    { 10,  7, 58, 30, 23, 62,
        7, 64, 62, 23, 62, 61,
        7, 41, 62, 21,  7, 49,
      75,  7, 69, 53, 58, 37,
      37, 41, 10, 64, 50,  7,
      10, 64, 21, 62, 61, 35,
      62, 61, 62,  7, 52, 10,
      21, 58,  7, 49, 75,  7,
      62, 26, 22, 53, 30, 21,
      10, 37, 64};

    decrypt(message, n, d);
    return 0;
}

void decrypt(vector<int> numText, int n, int d)
{
    char charText;
    long x;
    int m, C = 0;
    cout << "message: " << endl;
    for(int i = 0; i < numText.size(); i++)
    {
        C = numText.at(i);
        //cout << C << endl;
        /*x = pow(C, d);
        cout << x << endl;
        m = x%n;

        string str = to_string(m);
        cout << m << " ==> " << str << endl;*/
        m = static_cast<int>(pow(C,2)) % n;
        m = static_cast<int>(pow(m,3)) % n;
        m = (m*C) % n;

        if (m == 28) { cout << ' '; }
        else
        {
            m += 63;
            charText = m;
            cout << charText;
        }
    }
    cout << endl;
}
```


message:
I HAVE NEVER LET MY SCHOOLING INTERFERE WITH MY EDUCATION
Program ended with exit code: 0

Problem 3:

(a) Compute $13^{-1} \pmod{19}$ by enumerating multiples of the number and the modulus. Show your work. Referring to the slides in number theory. We want to find an integer a and b that satisfies $13^{-1} \pmod{19}$

$$\begin{aligned} a &= 13^{-1} \pmod{19} && \text{Multiply both sides by 13} \\ 13 \cdot a &= 1 \pmod{19} && \text{turn into multiple form} \\ 13 \cdot a &= 19 \cdot b + 1 \end{aligned}$$

On the LHS, we have multiples 13,26,29. On the RHS, we have multiples 20,39,58.
Since $39 = 19 \cdot 2 + 1$, we have $a = 3$ and $b = 2$.So as a result we have $13^{-1} = 3 \pmod{19}$.
Finally, substituting what we just found $13^{-1} \pmod{19} = 3 \pmod{19}$

(b) Compute $13^{-1} \pmod{19}$ using Fermat's theorem. Show your work.
Referring to the slides in number theory. We want to find use Fermat's little Theorem

$$\begin{aligned} a^{p-1} &= 1 \pmod{p} && \text{If p is a prime number, and a is not divisible by p(FLT)} \\ 13^{19-1} &= 1 \pmod{19} && \text{Multiplying, we get this} \\ 13^{18} &= 1 \pmod{19} \end{aligned}$$

Next we apply FLT to our equation. We will use what we just found above

$$\begin{aligned} 13^{18} \cdot 13^{-1} &= 1 \pmod{19} && \text{If p is a prime number, and a is not divisible by p(FLT)} \\ 13^{17} &= 1 \pmod{19} && \text{Multiplying, we get this} \end{aligned}$$

Listing out exponential and their remainders. This will help us get the final answer

$$\begin{aligned} 13^{2} &\pmod{19} = 17 \\ 13^{4} &\pmod{19} = 4 \\ 13^{8} &\pmod{19} = 16 \\ 13^{16} &\pmod{19} = 9 \end{aligned}$$

Applying what we just found

$$\begin{aligned} &13^{17} \pmod{19} = 13^{16} \cdot 13^{1} \pmod{19} && \text{We know that } 13^{16} \pmod{19} = 9 \\ &13^{16} \cdot 13^{1} \pmod{19} = 9 \pmod{19} \cdot 13 \pmod{19} \\ &9 \pmod{19} \cdot 13 \pmod{19} = 142 \pmod{19} \\ &117 \pmod{19} = 3 \end{aligned}$$

This matches our final answer in (a). Therefore $13^{-1} \pmod{19} = 3 \pmod{19}$

(c) Compute $13^{-40} \pmod{19}$ using Fermat's theorem. Show your work. For this equation

$$\begin{aligned} a^{p-1} &= 1 \pmod{p} && \text{If p is a prime number, and a is not divisible by p(FLT)} \\ 13^{19-1} &= 1 \pmod{19} && \text{Multiplying, we get this} \\ 13^{18} &= 1 \pmod{19} \end{aligned}$$

Next we apply FLT to our equation. We will use what we just found above

$$\begin{aligned}
13^{18} * 13^{-40} \pmod{19} &\equiv 13^{-22} \pmod{19} \\
13^{18} * 13^{-22} \pmod{19} &\equiv 13^{-4} \pmod{19} \\
13^{18} * 13^{-4} \pmod{19} &\equiv 13^{14} \pmod{19}
\end{aligned}$$

Listing out exponential and their remainders, will help us find answer for $13^{14} \pmod{19}$

$$\begin{aligned}
13^{2} \pmod{19} &= 17 \\
13^{4} \pmod{19} &= 4 \\
13^{8} \pmod{19} &= 16
\end{aligned}$$

$$\begin{aligned}
&13^{14} \pmod{19} = (13^{8} * 13^{4} * 13^{2}) \pmod{19} \\
&13^{14} = (16 * 4 * 17) \pmod{19} \\
&= (1088) \pmod{19} \\
&= 5 && \text{Final answer}
\end{aligned}$$

(d) Find a number $x \in \{1, 2, ..., 36\}$ such that $8x \equiv 3 \pmod{37}$. Show your work. (You need to follow the method covered in class; brute-force checking all values of x will not be accepted.)

$$\begin{aligned}
&8x \equiv 3 \pmod{37} && \text{Multiply both sides by the inverse of 8} \\
&8^{-1} \cdot 8x \equiv 3 \pmod{37} \cdot 8^{-1} \\
&x \equiv 3 \pmod{37} \cdot 8^{-1}
\end{aligned}$$

Solving for $8^{-1} \pmod{37}$

$$\begin{aligned}
&a = 8^{-1} \pmod{37} && \text{Multiply both sides by 8} \\
&8 \cdot a = 37 \cdot b + 1 && \text{turn into multiple form}
\end{aligned}$$

Listing out multiples on the RHS: 37,75,112. We know that 112 is divisible by 8.
Therefore we have $a = 14$ and $b = 3$.At the end we know that $8^{-1} \pmod{37} = 14 \pmod{37}$
Plugging it in and solving, we get

$$\begin{aligned}
&x = 3 \cdot 14 \pmod{37} && \text{Multiply} \\
&x = 42 \pmod{37} && \text{Get remainder} \\
&x = 5 && \text{Final answer}
\end{aligned}$$

Submission. To submit the homework, you need to upload the pdf file into gradescope by Friday, May 4 (noon).