Hanzhe Teng SID 500653093
Zhenxiao Qi SID 500654348

CS 111 ASSIGNMENT 2

due Thursday, October 26 (8AM)

Problem 1: (a) Let x, y be two positive integers. Suppose that p is a prime whose multiplicity in the factorization of x is equal a and whose multiplicity in the factorization of y is equal b. (Note: if p does not actually appear in a factorization, then its multiplicity is assumed to be 0.)

(i) If x is a divisor of y, then what is the relation between a and b? Give this relation and a brief justification.

(ii) If $d = \gcd(x, y)$, then what is the multiplicity of p in the factorization of d? Explain how the answer follows from part (i).

(b) Compute the greatest common divisor (give its numerical value) of the following two numbers x, y:

$$x = 3^4 \cdot 7^{321} \cdot 11^{9101} \cdot 23^3$$
$$y = 2^2 \cdot 3^9 \cdot 7^3 \cdot 13^{2129} \cdot 23^1$$

Show your work and explain how the answer follows from part (a.ii).

Solution 1:

(a) In the following reasoning, we assume that $x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $y = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, $d = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$, in which $p_1, p_2, \cdots, p_n$ are relatively prime. The multiplicity would be 0 if p_i does not actually appear in the factorization.

To clarify the notations, we assume that i and j are integers in the range of 1 to n. When we don't point out the exact subscript, then a, b, c, and p stands for any index.

(i) Since x is a divisor of y, then $\frac{y}{x} = p_1^{b_1 - a_1} p_2^{b_2 - a_2} \cdots p_n^{b_n - a_n}$ should be an integer. Recall p_i and p_j are relatively prime, then for any index i, the multiplicity $b_i - a_i$ should not be negative. Thus, we have $b_i \geq a_i$ is true for all $i = 1$ to n. Then for any factor p, we have the relation that $b \geq a$.

(ii) Since $d = \gcd(x, y)$, then d is the common divisor of x and y. Since $d = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$, recall the conclusion in (i), we have $c_i \leq a_i$ and $c_i \leq b_i$. Thus, we have $c_i = \min(a_i, b_i)$. Since this conclusion is true for all index i, then we can generally say $c = \min(a, b)$ is true.

(b) From the conclusion in (ii), we can easily compute the greatest common divisor of the following numbers.

$$\begin{aligned}
\gcd(x, y) &= 2^{\min(0,2)} \cdot 3^{\min(4,9)} \cdot 7^{\min(321,3)} \cdot 11^{\min(9101,0)} \cdot 13^{\min(0,2129)} \cdot 23^{\min(3,1)} \\
&= 2^0 \cdot 3^4 \cdot 7^3 \cdot 11^0 \cdot 13^0 \cdot 23^1 \\
&= 81 \cdot 343 \cdot 23 \\
&= 639009
\end{aligned}$$

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:

- Give Bob's message in plaintext (also, what does it mean and who said it?).
- Describe step by step how you arrived at the solution.
- show your work (the computation) for the first three numbers in the message.

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

Solution 2:

First, let's "break" RSA by guessing the factorization of n, which is 77 in this problem. Easy to get the prime factors $p = 7$ and $q = 11$. Then we can compute Euler's Totient Function $\varphi(n) = (p-1) \cdot (q-1) = 6 \cdot 10 = 60$.

Since the selected encryption exponent e is 13, we can get the decryption exponent d by computing $e^{-1} \pmod{\varphi(n)}$, which is $13^{-1} \pmod{60}$ in this problem. We solve this by enumerating.

To compute $13^{-1} \pmod{60}$ is to compute $13 \cdot a \equiv 1 \pmod{60}$. It also means to find the proper a and b to satisfy $13 \cdot a = 60 \cdot b + 1$. So we can enumerate both sides.

Left side: 13 26 39 52 65 78 91 104 117 130 143 156 169 182 195 208 221 234 247 260 273 286 299 312 325 338 351 364 377 390 403 416 429 442 455 468 481

Right side: 61 121 181 241 301 361 421 481

So we can see that they are equal to 481 when $a = 37$ and $b = 8$. Thus, we have decryption exponent $d = 37$ and the private key pair $(d, n) = (37, 77)$. Then we can decrypt the following messages by $M = C^d \pmod{n} = C^3 7 \pmod{77}$, in which M stands for the original messages and C stands for the encrypted messages.

We only give the detailed decryption solution for the first three cases. For the rest cases, we solve them by a python program, which is appended to the end of this homework file.

Computed by program, we finally have all the decoded numbers [10, 28, 9, 2, 23, 6, 28, 15, 6, 23, 6, 19, 28, 13, 6, 21, 28, 14, 26, 28, 20, 4, 9, 16, 16, 13, 10, 15, 8, 28, 10, 15, 21, 6, 19, 7, 6, 19, 6, 28, 24, 10, 21, 9, 28, 14, 26, 28, 6, 5, 22, 4, 2, 21, 10, 16, 15] and Bob's message "I HAVE NEVER LET MY SCHOOLING INTERFERE WITH MY EDUCATION".

$$
\begin{aligned}
\text{For } \ C = 10, M &= 10^{37} \pmod{77} \\
&= 10 \cdot 100^{18} \pmod{77} \\
&= 10 \cdot 23^{18} \pmod{77} \\
&= 10 \cdot 529^{9} \pmod{77} \\
&= 10 \cdot (462 + 67)^{9} \pmod{77} \\
&= 10 \cdot 67^{9} \pmod{77} \\
&= 10 \cdot 67 \cdot (67^{2})^{4} \pmod{77} \\
&= 670 \cdot 4489^{4} \pmod{77} \\
&= (616 + 54) \cdot (4466 + 23)^{4} \pmod{77} \\
&= 54 \cdot 23^{4} \pmod{77} \\
&= 54 \cdot 529^{2} \pmod{77} \\
&= 54 \cdot 67^{2} \pmod{77} \\
&= 54 \cdot 4489 \pmod{77} \\
&= 54 \cdot 23 \pmod{77} \\
&= 10
\end{aligned}
$$

$$
\begin{aligned}
\text{For } \ C = 7, M &= 7^{37} \pmod{77} \\
&= 7 \cdot 49^{18} \pmod{77} \\
&= 7 \cdot 2401^{9} \pmod{77} \\
&= 7 \cdot 14^{9} \pmod{77} \\
&= 7 \cdot 2744^{3} \pmod{77} \\
&= 7 \cdot 49^{3} \pmod{77} \\
&= 7 \cdot 49 \cdot 2401 \pmod{77} \\
&= 7 \cdot 49 \cdot 14 \pmod{77} \\
&= 28
\end{aligned}
$$

$$
\begin{aligned}
\text{For } \ C = 58, M &= 58^{37} \pmod{77} \\
&= 58 \cdot 3364^{18} \pmod{77} \\
&= 58 \cdot 53^{18} \pmod{77} \\
&= 58 \cdot 2809^{9} \pmod{77} \\
&= 58 \cdot 37^{9} \pmod{77} \\
&= 58 \cdot 50653^{3} \pmod{77} \\
&= 58 \cdot 64^{3} \pmod{77} \\
&= 58 \cdot 64 \cdot 4096 \pmod{77} \\
&= 58 \cdot 64 \cdot 15 \pmod{77} \\
&= 9
\end{aligned}
$$

Problem 3:

(a) Compute $13^{-1} \pmod{19}$ by enumerating multiples of the number and the modulus. Show your work.

(b) Compute $13^{-1} \pmod{19}$ using Fermat's theorem. Show your work.

(c) 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.)

Solution 3:

(a) To compute $13^{-1} \pmod{19}$ is to compute $13 \cdot a \equiv 1 \pmod{19}$. It also means to find the proper a and b to satisfy $13 \cdot a = 19 \cdot b + 1$. So we can enumerate both sides to see when it will be equal.

Left side: 13 26 39 52 65 78 91 104 117 130

Right side: 20 39 58 77 96 115 134 153

So we can see that they are equal to 39 when $a = 3$ and $b = 2$. Thus, the inverse of 13 is 3 when module 19.

(b) From Fermat's theorem we have $13^{18} \equiv 1 \pmod{19}$, then we can just implement it to computation.

$$\begin{aligned}
13^{-1} \pmod{19} &\equiv 13^{-1} \cdot 13^{18} \pmod{19} \\
&\equiv 13^{17} \pmod{19} \\
&\equiv (13^2)^8 \cdot 13 \pmod{19} \\
&\equiv 169^8 \cdot 13 \pmod{19} \\
&\equiv (152 + 17)^8 \cdot 13 \pmod{19} \\
&\equiv 17^8 \cdot 13 \pmod{19} \\
&\equiv (17^2)^4 \cdot 13 \pmod{19} \\
&\equiv 289^4 \cdot 13 \pmod{19} \\
&\equiv (285 + 4)^4 \cdot 13 \pmod{19} \\
&\equiv 4^4 \cdot 13 \pmod{19} \\
&\equiv 256 \cdot 13 \pmod{19} \\
&\equiv (247 + 9) \cdot 13 \pmod{19} \\
&\equiv 9 \cdot 13 \pmod{19} \\
&\equiv 117 \pmod{19} \\
&\equiv 3 \pmod{19}
\end{aligned}$$

So the answer of $13^{-1} \pmod{19}$ is 3.

(c) First, we have to compute $8^{-1} \pmod{37}$. We do this by enumerating. To compute $8^{-1} \pmod{37}$ is to compute $8 \cdot a \equiv 1 \pmod{37}$. It also means to find the proper a and b to satisfy $8 \cdot a = 37 \cdot b + 1$. So we just enumerate both sides.

Left side: 8 16 24 32 40 48 56 64 72 80 88 96 104 112

Right side: 38 75 112

So we can see that they are equal to 112 when $a = 14$ and $b = 3$. Thus, $8^{-1} \pmod{37} \equiv 14$.

Recall the problem, we want to solve $8x \equiv 3 \pmod{37}$. For now we can solve it by $x \equiv 3 \cdot 14 \pmod{37} \equiv 42 \pmod{37} \equiv 5 \pmod{37}$. So the answer is 5 when $x \in \{1, 2, ..., 36\}$.

CS 111 Problem Two Python Program

by Hanzhe Teng and Zhenxiao Qi, Oct 26, 2017

```
def fastMod(b, e, m):
    t = 1
    while e != 0:
        if (e&1) == 1:
            t = (t * b) % m
        e >>= 1
        b = (b*b) % m
    return t

def Euclid(y1,y2):
    a=[1,0,y1]
    b=[0,1,y2]
    c=[]
    while(b[2]!=1):
        a=a[2]/b[2]
        for i in range(2):
            c[i]=a[i]-q*b[i]
        for i in range(3):
            a[i]=b[i]
            b[i]=c[i]
    return b[1]


def computeD(fn, e):
    (x, y, r) = Euclid(fn, e)
    if y < 0:
        return fn + y
    return y


def decryption(C, d, n):
    return fastMod(C, d, n)

data= [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]

M = []
plaintext=""
for i in range(len(data)):
   M.append(decryption(data[i], 37, 77))
for i in range(len(M)):
    if (M[i]==28):
        plaintext+=" "
    else: plaintext+=chr(M[i]+63)
print(M)
print (plaintext)
```