INF240 Mandatory Exercise 2

David Huynh
E-mail: dhu009@student.uib.no

1 Computer Problem 14, Chapter 6

There are three users with pairwise relatively prime moduli n_1, n_2, n_3. Suppose that their encryption exponents are all $e = 3$. The same message m is sent to each of them and you intercept the ciphertexts $c_i \equiv m^3 (mod\ n_i)$ for i = 1,2,3.

1.1 A)

Show that $0 \leq m^3 < n_1 n_2 n_3$

Solution:
$m < n_1, n_2, n_3 \rightarrow m^3 < n_1 n_2 n_3$

1.2 B)

Show how to use the Chinese remainder theorem to find m^3 (as an exact integer, *not* only as $m^3 (mod\ n_1 n_2 n_3)$) and therefore m. Do this without factoring

Solution:
We setup the problem as a system of linear congruences:

$c_1 \equiv m^3 (mod\ n_1)$
$c_2 \equiv m^3 (mod\ n_2)$
$c_3 \equiv m^3 (mod\ n_3)$

This can be written as:
$m^3 \equiv c_1 (mod\ n_1)$
$m^3 \equiv c_2 (mod\ n_2)$
$m^3 \equiv c_3 (mod\ n_3)$

By Chinese Remainder Theorem there exists one unique solution.
From **??** we know that $m < n_1, n_2, n_3$ and $m^3 < n_1 n_2 n_3$.
We can thus find m by taking the cube root of m^3. $m = \sqrt[3]{m^3}$

1.3 C)

Suppose that
$n_1 = 2469247531693$, $n_2 = 11111502225583$, $n_3 = 44444222221411$
and the corresponding ciphertexts are:
359335245251, 10436363975495, 5135984059593.

These were all encrypted using $e = 3$. Find the message.

Solution:
Solve the system of congruences from **??** using CRT to obtain m^3. I used the algorithm described on page 108, problem 24 in our book to solve it.
First we compute the product of $n_1n_2n_3 = 1219418322585514865441452950268831928809$
Then we obtain the values z_i by computing $(n_1n_2n_3)/n_i$ for $i = 1$ to 3.
Afterwards we compute the multiplicative inverse of $y_i = z_i \bmod n_i$ for $i = 1$ to 3
Lastly we sum together $a_i * y_i * z_i$ for $i = 1$ to 3 and reduce modulo $(n_1n_2n_3)$, this is m^3
$m^3 = 521895811536685104609613375$
$m = \sqrt[3]{m^3} = \sqrt[3]{521895811536685104609613375} = 805121215$
Replace each pair of numbers (08, 05, 12...) with the english letter at that position, where a = 01, b = 02... to find the decrypted message
Decrypted message = hello

Program output:

```
The product of n1n2..nk is: 1219418322585514865441452950268831928809
z1 for n1 : 493842074127513750694557613
y1 for n1 : 216851051457

z2 for n2 : 109743786018234293085678823
y2 for n2 : 2933660999772

z3 for n3 : 27437049443922098827902019
y3 for n3 : 28806927150227

M^3 = 521895811536685104609613375
M = 805121215
Decrypted message: hello
```