Programming Assignment 2

Darin Goldstein

1 Deadline

3/5/2020

2 Complex multiplication problems

Define a k-grouping of n numbers in the world of (mod p) to be a set of exactly k of the n numbers multiplied together (mod p). For example, one possible 3-grouping of the numbers $2, 4, 7, 9$ in the world of (mod 11) is 6 because 2 times 4 times 9 is 72, which is 6 in the world of (mod 11). There are $\binom{n}{k}$ k-groupings of n numbers.

Assume that there are $N-1$ integers $a_1, a_2, \ldots, a_{N-1}$ in the world of (mod p) where p is a large prime number (smaller than 32 bits) and N is a power of 2. A company wants to hire you to compute the sum of all possible k-groupings of these numbers $a_1, \ldots, a_{N-1}$ in the world of (mod p). However, they do not have the values of the numbers $a_1, \ldots, a_{N-1}$. Instead, for some r, they have the following values:

$$\forall 0 \leq j < N, (r^j + a_1)(r^j + a_2) \ldots (r^j + a_{N-1}) (\text{mod } p)$$

or, if you prefer to write the same thing a different way, they have the values $\forall 0 \leq j < N, \prod_{k=1}^{N-1}(r^j + a_k) \pmod{p}$.

After some study, you happen to notice by incredible coincidence that $r^N \equiv 1 \pmod{p}$ and $\forall 1 \leq j < N, r^j \not\equiv 1 \pmod{p}$. By another amazing coincidence, you also happen to notice that

$$\sum_{j=0}^{N-1} r^j \equiv 0 (\text{mod } p)$$

This sparks you to remember a potentially helpful algorithm...

Given the values of p, r, and the N integers $\forall 0 \leq j < N, \prod_{k=1}^{N-1}(r^j + a_k)$ as input, one integer per line, you will output the sum of the k-groupings of the numbers, one per line, modulo p, for $k = 1$ (first) through $N-1$ (last).

2.1 Example

Assume that $p = 53$ and $r = 30$. The input might be (assuming that $a_1 = 6, a_2 = 13, a_3 = 30$)

$53 = p$
$30 = r$
$17 = (1 + 6)(1 + 13)(1 + 30) \bmod 53$
$24 = (30 + 6)(30 + 13)(30 + 30) \bmod 53$
$44 = (30^2 + 6)(30^2 + 13)(30^3 + 30) \bmod 53$
$0 = (30^3 + 6)(30^3 + 13)(30^3 + 30) \bmod 53$

IMPORTANT: The input will not look exactly like this. It will only have a single number per line. The equations are there to show you how the numbers were computed.

The output should be

$49 = 6 + 13 + 30 \bmod 53$
$12 = 6 \cdot 13 + 6 \cdot 30 + 13 \cdot 30 \bmod 53$
$8 = 6 \cdot 13 \cdot 30 \bmod 53$

IMPORTANT: Again, the output will not look exactly like this. It will only have a single number per line. The equations are there to show you how the numbers were computed.

Please refer to the example files for formatting issues.