

# On Certain Lehmer Generators

We are interested in Lehmer generators of pseudorandom numbers.

Let  $x_{n+1} = R \cdot x_n \pmod{M}$  be a Lehmer generator and let  $M$  be a prime in some interval  $[A, B]$ .

It is known that the length of the sequence period of this generator is maximal when  $R$  is a primitive root modulo  $M$ . To construct the appropriate generator we have to find at least some primitive roots modulo  $M$ .

A primitive root  $R$  modulo  $M$  can be characterized in two ways.

1. Every positive integer less than  $M$  is congruent to some power of  $R$  modulo  $M$ . This is in fact a standard definition.
2. Let  $PFM$  be the set of all prime factors of  $M-1$ . Then  $R$  is the primitive root of  $M$  if and only if  
 $R^{(M-1)/p}$  is not congruent to 1 mod  $M$ , for all  $p \in PFM$ .

The second characterization is especially useful for a fast computational test whether a given number is a primitive root modulo  $M$ .

For various number theoretic reasons, we prefer to work with primitive roots which are relatively highly composite, that is, which have many divisors. An integer is called  $F$ -composite if its number of divisors is at least  $F$ .

When prime  $M$  is huge the number of primitive roots modulo  $M$  is also huge and even the number of highly composite primitive roots modulo  $M$  might be quite substantial. Consequently, we restrict our search for primitive roots modulo  $M$  even more. We are going to look for  $F$ -composite primitive roots modulo  $M$  only in some given interval  $[C, D]$ .

Let us denote by  $S_{ABCDEF}$  the set of all primes  $M$  with the property that  $M \in [A, B]$  and that the number of  $F$ -composite primitive roots modulo  $M$  in interval  $[C, D]$  is at least  $E$ .

## The task

Given the values of  $A, B, C, D, E, F$ , find the set  $S_{ABCDEF}$ .

### Input

The input contains one line with six integers  $A, B, C, D, E, F$  separated by space. It holds:

$$1 < C < D < A < B < 10^{15}, \quad 1 < E, F < 200, \quad B - A \leq 2500, D - C \leq 2500.$$

### Output

The output consists of one line with two integers  $N, P$  separated by space.  $N$  is the cardinality of  $S_{ABCDEF}$ ,  $P$  is equal to the product of all primes in  $S_{ABCDEF}$  expressed modulo sum of all primes in  $S_{ABCDEF}$ . You may suppose that  $S_{ABCDEF}$  is unempty and that  $N \leq 200$  for all input data in this problem.

## Example 1

### Input

```
30 50 10 25 3 6
```

### Output

```
2 71
```

The resulting two primes in interval  $[30, 50]$  (and their respective 6-composite primitive roots in interval  $[10, 25]$ ) are 37 (18, 20, 24) and 43 (12, 18, 20). The product of the primes is 1591, the sum of primes is  $80 \cdot 1591 \pmod{80} = 71$ .

## Example 2

### Input

```
50 100 15 45 2 8
```

### Output

```
4 81
```

The resulting four primes in interval  $[50, 100]$  (and their respective 8-composite primitive roots in interval  $[15, 45]$ ) are 59 (24, 30, 40, 42), 73 (40, 42), 83 (24, 42), 89 (24, 30).

The product of the primes is 31815809, the sum of primes is  $304 \cdot 1815809 \pmod{304} = 81$ .

## Example 3

### Input

```
200000000001 20000002222 19900007777 19900009999 50 70
```

### Output

## Public data

The public data set is intended for easier debugging and approximate program correctness checking. The public data set is stored also in the upload system and each time a student submits a solution it is run on the public dataset and the program output to stdout and stderr is available to him/her.

[Link to public data set](#)