$$0 \leq x_0 < M,$$
$$x_{n+1} = (Ax_n + C) \mod M, \quad n \geq 0.$$

$$M = (p_1 p_2 \ldots p_F)^2$$

0. Generate primes up to Pmax
1. Generate all possible M's:

```
public static void generateFactors(int index, long prod) {
        long m = prod*primes[index];
        if (m > sqrt_of_maxM)
            return;
        … [TODO] check if m*m is the searched M
        generateFactors(index+1, m); // skip primes[index]
        generateFactors(index+1, prod); // include primes[index]
    }
```

2. For each generated M, calculate A and C from the given sequence
3. Check the constraints of Hull-Dobell theorem, ensure that (A, C, M) generates the whole sequence

Safe multiplication for large numbers

```
static long moduloMult(long a, long b, long mod) {
        long res = 0; // Initialize result
        a %= mod;
        while (b > 0) {
                if ((b & 1) > 0) // If b is odd, add ‘a’ to result
                        res = (res + a) % mod;
                a = (2 * a) % mod;
                b >>= 1; // b = b / 2
        }
        return res;
  }
```