

Computational Number Theory

Programming HW 4

Due Date: 26/10/2025

Input: The input is a csv file with the first line having a prime p that is less than 10^7 . Each subsequent line is of the form $d, a_d, a_{d-1}, \dots, a_0$. This represents a square-free polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$ in $\mathbb{Z}_p[x]$, and the goal is to factorize $f(x)$.

The number of test cases will be at most 5 and the value of d will be in $\{2, \dots, 30\}$. All instances will have the leading coefficient as 1. A sample input file is attached.

Output: For each polynomial $f(x) \in \mathbb{Z}_p[x]$, print each of its irreducible factors as a sequence of coefficients on one line.

Output for the given sample input file (input-CZ.csv):

```
(x + 1) * (x^2 + 987012*x + 987012) * (x^3 + 987012*x + 987010) * (x^4 + 987011)

(x^6 + 63434*x^5 + 53353*x^4 + 13530*x^3 + 22643*x + 57541) *
(x^6 + 119366*x^5 + 749238*x^4 + 681331*x^3 + 613428*x^2 + 420559*x + 716564) *
(x^6 + 420745*x^5 + 820563*x^4 + 601116*x^3 + 225233*x^2 + 163860*x + 847631) *
(x^6 + 473938*x^5 + 630954*x^4 + 824457*x^3 + 356777*x^2 + 81717*x + 627235)

(x + 1) * (x + 987012) * (x^2 + 987012*x + 987012) *
(x^4 + 98011) * (x^4 + 987012*x + 987009) *
(x^6 + 63434*x^5 + 53353*x^4 + 13530*x^3 + 22643*x + 57541)
```

Note that it is okay to have a different output formatting, for example, in the same format as input. In this case, the second output may look like:

```
6,1,473938,630954,824457,356777,81717,627235
6,1,63434,53353,13530,0,22643,57541
6,1,119366,749238,681331,613428,420559,716564
6,1,420745,820563,601116,225233,163860,847631
```

Note also that there is no particular ordering among the factors of same degree. Also you can test Phase 1 (distinct degree factorization), and Phase 2 (same degree factorization) algorithms using inputs 1 and 2 respectively.