Computational Number Theory
Programming HW 4

Due Date: 07/04/2024

Input: The input is a csv file with three lines, the first line having a prime p that is less than 10^7. The second and third lines are each of the form $d, a_d, a_{d-1}, \ldots, a_0$ with $1 \leq d \leq 30$. This represents a polynomial $a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ in $\mathbb{Z}_p[x]$, of degree d; thus a_d will be non-zero. Let the two polynomials on line 2,3 be $f(x), g(x)$.

Output:

(a) $gcd(f(x), g(x))$;

(b) $u(x), v(x)$ such that $f(x)u(x) + g(x)v(x) = gcd(f(x), g(x))$.

Output for the first sample input file (input-polygcd1.csv):

```
GCD: x^2 + 2
u: 10*x + 9
v: 21
```

Output for the second sample input file (input-polygcd2.csv):

```
GCD: 1
u: 1374*x^7 + 1303*x^6 + 175*x^5 + 1681*x^4 + 49*x^3 + 931*x^2 + 217*x + 247
v: 1535*x^7 + 1533*x^6 + 1801*x^5 + 672*x^4 + 1865*x^3 + 1135*x^2 + 1110*x + 1520
```