

MATH 343, PROBLEM SET 1

ANDREW J. BLUMBERG

1. PROBLEMS

- (1) Write a computer program that computes $\gcd(x, y)$ using the Euclidean algorithm. Read the numbers from a file “input.txt”, which will have x on the first line and y on the second line. Output the result to a file “output.txt”.
- (2) Write a computer program that computes addition and multiplication in the ring \mathbb{Z}/m . The input is a file “input.txt” that has m on the first line, either $+$ or $*$ on the second line, and then x and y on the subsequent lines. Output the result to a file “output.txt”.
- (3) Write a computer program that computes g^x for $g \in \mathbb{Z}/n$ and $x \in \mathbb{Z}$ using the fast exponentiation algorithm. The input is a file “input.txt” that has n on the first line, g on the second line, and x on the third. Output the result to a file “output.txt”.
- (4) Write a program that decodes an encrypted message about which you know only that it was encoded using some shift cipher. The input is a file “input.txt” that just has the message text. Output the result to a file “output.txt”.
- (5) From the text: 1.14, 1.23, 1.25.