

Cryptography

ECE 5632

Sheet 1

Spring 2025

Problem 1

Calculate the following:

- (a) $15 \times 29 \pmod{13}$
- (b) $2 \times 29 \pmod{13}$
- (c) $2 \times 3 \pmod{13}$
- (d) $-11 \times 3 \pmod{13}$

Problem 2

Calculate the multiplicative inverse of 4 in $\mathbf{Z}_5, \mathbf{Z}_{11}, \mathbf{Z}_{12}, \mathbf{Z}_{13}$.

Problem 3

Based on your results in Problem 2, calculate the following:

- (a) $1/4 \pmod{11}$
- (b) $3/4 \pmod{5}$
- (c) $3 \times 2/4 \pmod{5}$

Problem 4

Calculate the following:

- (a) $7^2 \pmod{13}$
- (b) $7^{10} \pmod{13}$
- (c) $7^{100} \pmod{13}$

Problem 5

For the Affine cipher with encryption function, $y = (ax + b) \pmod{26}$.

- (a) What are the limitations on the values of a , and b ?
- (b) What is the key space for this cipher?

Problem 6

A ciphertext has been generated with an Affine cipher as in Problem 5. The first and second most frequent letters in the ciphertext are B and U, respectively. If the plaintext was an English text, break this cipher.