

2 Modular Arithmetic

2.1

Solve the following modular arithmetic questions

1. $(13 \bmod 3) + (23 \bmod 4)$
2. $(22 \bmod 7) \times (13 \bmod 7)$
3. $(14 \bmod 55 + 42 \bmod 55) \times (13 \bmod 55)$
4. $11 \div 7 \pmod{13}$
5. $4 \div 11 \pmod{17}$

2.2

For each number below, give its modular inverse (if defined) under a modulus of 8

- | | |
|----------------------|----------------------|
| 1. $0^{-1} \pmod{8}$ | 5. $4^{-1} \pmod{8}$ |
| 2. $1^{-1} \pmod{8}$ | 6. $5^{-1} \pmod{8}$ |
| 3. $2^{-1} \pmod{8}$ | 7. $6^{-1} \pmod{8}$ |
| 4. $3^{-1} \pmod{8}$ | 8. $7^{-1} \pmod{8}$ |

2.3

If multiplication distributes over subtraction under modulus then, which of the following statements are true

1. $a(b - c) \equiv a - bc \pmod{n}$
2. $a(b - c) \equiv ab - ac \pmod{n}$
3. $a(b - c) \equiv ac - ab \pmod{n}$
4. $a - bc \equiv ab - ac \pmod{n}$

2.4

What is the additive inverse of:

1. 24
2. $5 \pmod{17}$
3. $a \bmod b$ (give your answer as a formula)

2.5

Write the following as products of their prime factors in the form $f_1 \times f_2 \times f_3 \times \dots$

- | | |
|--------|-------|
| 1. 68 | 3. 92 |
| 2. 123 | 4. 44 |

2.6

Assume a string is encrypted using the encryption function $E(X) = (aX + b) \bmod n$, where X is the index of an element drawn from the alphabet [abcdefghijklmnopqrstuvwxyz0123456789], and n is the length of that alphabet.

1. Encrypt the string “hello” with keys $a=7$, $b=4$
2. Decrypt the string “q4zajep” with the same keys

2.7

Assume $p = 23$, $g = 7$. Alice generates a public key $A = 11$ using the following formula: $A = g^a \bmod p$, where A is the public key and a is a private key.

1. Find a value for Alice’s private key by brute force
2. You pick a private key $b = 11$. Calculate your public key, $B = g^b \bmod p$
3. A shared secret s can be calculated with the formula $s = A^b \bmod p$, where A is Alice’s public key, and b is your private key. Find s .

2.8

The following strings have been encrypted using the function $E(X_i) = (X + k + i) \bmod 26$, where i is the 1-based index of the character in the word to encrypt (ignoring spaces). For each, give a value for k .

1. “kxabcqph” (The first letter of plaintext is ‘c’)
2. “lacn ep gs” (The plaintext is a sentence)

2.9

VCKIVHH GSV UFMXGRLM FHVW GL VMX-IBKG GSRH GVC G FHRMT Z ULINFOZ