

M360 Mathematics of Information Security

homework sheet # 1

Problem # 1

Let $a, b, c, d, k \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{0\}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then show that

- (a) $a + c \equiv b + d \pmod{n}$
- (b) $ac \equiv bd \pmod{n}$
- (c) $a + k \equiv b + k \pmod{n}$
- (d) $ak \equiv bk \pmod{n}$.

Problem # 2

Caesar wants to arrange a secret meeting with Marc Anthony either at the Tiber (the *river*) or at the Coliseum (the *arena*). He sends the ciphertext *EVIRE*. However, Anthony does not know the key, so he tries all possibilities. Where will he meet Caesar? (*Hint*: This is a trick question).

Problem # 3

The ciphertext UCR was encrypted using the affine function $9x + 2 \pmod{26}$. Find the plaintext.

Problem # 4

Encrypt *howareyou* using the affine function $5x + 7 \pmod{26}$. What is the decryption function? Check that it works.

Problem # 5

Consider an affine cipher (mod 26). You do a chosen plaintext attack using *hahaha*. The ciphertext is *NONONO*. Determine the encryption function.

Problem # 6

The following ciphertext was encrypted by an affine cipher mod 26: *CRWWZ*. The plaintext starts *ha*. Decrypt the message.

Problem # 7

Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

Problem # 8

Suppose you work mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if you work mod 29?

Problem # 9

- (a) Find integers x and y such that $17x + 101y = 1$.
- (b) Find $17^{-1} \pmod{101}$.

Problem # 10

- (a) Solve $1d \equiv 1 \pmod{30}$
- (b) Suppose you write a message as a number $m \pmod{31}$. Encrypt m as $m^7 \pmod{31}$. How would you decrypt? (*Hint*: Decryption is done by raising the ciphertext to a power mod 31. Fermat's theorem will be useful.)

Problem # 11

- (a) Find all solutions of $12x \equiv 28 \pmod{236}$
- (b) Find all solutions of $12x \equiv 30 \pmod{236}$

Problem # 12

- (a) Use the Euclidean algorithm to compute $\gcd(30030, 257)$
- (b) Using the result of part (a) and the fact that $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, show that 257 is prime.

Problem # 13

- (a) Compute $\gcd(4883, 4369)$
- (b) Factor 4883 and 4369 into products of primes.

Problem # 14

- (a) Let $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ define the Fibonacci sequence $1, 1, 2, 3, 5, 8, \dots$. Use the Euclidean algorithm to compute $\gcd(F_n, F_{n-1})$ for all $n \geq 1$.
- (b) Find $\gcd(11111111, 11111)$.
- (c) Let $a = 111 \cdots 11$ be formed with F_n repeated 1's and let $b = 111 \cdots 11$ be formed with F_{n-1} repeated 1's. Find $\gcd(a, b)$.

Problem # 15

When picking 2 successive cards from a standard 52-card deck, what is the probability of:

- a) The first card is an Ace and the second card is not a Queen?
- b) The first card is Spade and the second card is not a Queen?

Problem # 16

There are 50 cards numbered from 1 to 50. Two different cards are chosen at random. What is the probability that one number is twice the other number?

Problem # 17

- a) Compute the gcd of 122 and 48 and write it in the form $s \cdot 122 + t \cdot 48$ with $s, t \in \mathbb{Z}$.
- b) Solve the equation $10x + 15y + 12z = 1$ with integers x, y, z .
- c) Show that the equation $12x + 15y + 21z = 1$ does not have a solution with integers x, y, z .

Bonus: For a, b, c and d integers, under which conditions does the equation $ax + by + cz = d$ has integer solutions in x, y, z .

not collected.