MATH 4282 – Cryptography Assignment #3
Winter 2019

Instructions

- Answer each question completely; justify your answers.

Definition: A *field* $(\mathcal{F}, +, \cdot)$ consists of a set $\mathcal{F}$ along with two binary operations, $+$ and $\cdot$, such that:

- $\mathcal{F}$ is closed under both $+$ and $\cdot$
- $+$ and $\cdot$ are both commutative (i.e., $a + b = b + a$ and $a \cdot b = b \cdot a$)
- $+$ and $\cdot$ are both associative (i.e., $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- $\cdot$ distributes over $+$ (i.e., $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$)
- there exists an element $1 \in \mathcal{F}$ such that $a \cdot 1 = a$ for all $a \in \mathcal{F}$
- there exists an element $0 \in \mathcal{F}$ such that $a + 0 = a$ for all $a \in \mathcal{F}$
- for each $a \in \mathcal{F}$ there exists an element $(-a) \in \mathcal{F}$ such that $a + (-a) = 0$
- for each $a \in \mathcal{F}$ such that $a \neq 0$, there exists an element $a^{-1} \in \mathcal{F}$ such that $a \cdot a^{-1} = 1$

Note that when there is no confusion concerning $+$ and $\cdot$, we often refer to the field as $\mathcal{F}$ rather than $(\mathcal{F}, +, \cdot)$.

1. Determine whether each of the following is a field. Justify your answers.

   (a) $\mathbb{Z}$, using standard arithmetic

   (b) $\mathbb{Q}$, using standard arithmetic

   (c) $\mathbb{Z}_{26}$, using modular arithmetic (modulo 26)

   (d) $\mathbb{Z}_p$, where p is prime, using modular arithmetic (modulo p)

   (e) $\{0\}$, using standard arithmetic

Fact: A matrix M over a field $\mathcal{F}$ is invertible if and only if the rows of M are linearly independent.

2. Exercise 1.12 of Stinson: Let p be a prime. Show that the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$.

3. By $\mathbb{Z}_n^*$ we denote the set $\{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. A *quadratic residue* modulo n is any element x of $\mathbb{Z}_n^*$ that is a square (i.e., $x = y^2$ for some $y \in \mathbb{Z}_n^*$). What are the quadratic residues for

   (a) $\mathbb{Z}_{23}^*$

   (b) $\mathbb{Z}_{26}^*$

   (c) $\mathbb{Z}_{27}^*$

   In a few weeks we will see in class how to determine whether a given element $x \in \mathbb{Z}_p^*$ is a quadratic residue, where p is a prime. For instance, we'll learn how to answer the question: Is 789 a quadradic residue in $\mathbb{Z}_{5683}^*$?

(over)

A *group* $(\mathcal{G}, \cdot)$ consists of a set $\mathcal{G}$ along with a binary operation $\cdot$, such that:

- $\mathcal{G}$ is closed under $\cdot$
- $\cdot$ is associative (i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- there exists an identity with respect to $\cdot$
  (i.e., there exists an element $e \in \mathcal{G}$ such that $a \cdot e = e \cdot a = a$ for all $a \in \mathcal{G}$)
- each element has an inverse
  (i.e., for each $a \in \mathcal{G}$ there exists an element $b \in \mathcal{G}$ such that $a \cdot b = b \cdot a = e$)

Note that we often refer to the group as $\mathcal{G}$ rather than $(\mathcal{G}, \cdot)$. Notice also that $\cdot$ need not be commutative; a group in which $\cdot$ is commutative is called an *Abelian* group.

The notation a^n will be used to denote $\underbrace{a \cdot a \cdot a \cdots a}_{n\ a\text{'s}}$. The *order* of an element $a \in \mathcal{G}$ is the smallest positive integer t such that $a^t = e$. If a has order $|\mathcal{G}|$ then a is a *generator* of $\mathcal{G}$.

4. Find all generators of each of the following groups:
   (a) $\mathbb{Z}_{17}^*$
   (b) $\mathbb{Z}_{25}^*$

5. Prove the following statement:
   If the order of $a \in \mathbb{Z}_n^*$ is t and $a^s \equiv 1 \pmod{n}$, then t divides s.

6. (a) Suppose that α is a generator of $\mathbb{Z}_n^*$. Prove that α^k is a generator of $\mathbb{Z}_n^*$ if and only if $\gcd(k, \phi(n)) = 1$, where ϕ is Euler's totient function.
   (b) Provided that $\mathbb{Z}_n^*$ has at least one generator, then how many generators does it have?
   (c) When p is prime, $\mathbb{Z}_p^*$ is known to have a generator. How many generators are there in:
      i. $\mathbb{Z}_{31}^*$
      ii. $\mathbb{Z}_{181}^*$
      iii. $\mathbb{Z}_{257}^*$
      iv. $\mathbb{Z}_{2^t+1}^*$, where $(2^t + 1)$ is prime
      v. $\mathbb{Z}_{2t+1}^*$, where t and $(2t + 1)$ are prime

7. Solve for x by using Shanks' Algorithm:
   (a) $13^x \equiv 12 \pmod{197}$
   (b) $14^x \equiv 519 \pmod{557}$
   (c) $7^x \equiv 922 \pmod{1433}$