MATH 102 – HOMEWORK ASSIGNMENT 5

Due Friday, November 3rd, 2017 before the lecture.
Handwritten submissions only.

Exercise 1 (4 points)**.**
Compute the following determinants:

$$\begin{vmatrix} 2 & 3 & -1 \\ 0 & 3 & 1 \\ 1 & 2 & -3 \end{vmatrix}, \quad \begin{vmatrix} 1 & 5 & 1 \\ 2 & 1 & -1 \\ 4 & 2 & 1 \end{vmatrix}, \quad \begin{vmatrix} 2 & 2 & 8 \\ 5 & 2 & 2 \\ 1 & 1 & 4 \end{vmatrix}, \quad \begin{vmatrix} 6 & 1 & 3 \\ 4 & 4 & 2 \\ 10 & -5 & 5 \end{vmatrix}.$$

Exercise 2 (4 points)**.**
Compute the following determinants. Think before you start.

$$\begin{vmatrix} 0 & 0 & 3 & 0 & 0 \\ 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{vmatrix}, \quad \begin{vmatrix} -2 & 3 & 7 & 5 \\ 2 & -4 & -7 & 0 \\ 0 & -1 & -2 & 0 \\ 0 & 0 & -5 & 0 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & -1 & 0 & 2 \\ 0 & -4 & 0 & 1 & 0 \\ 5 & 0 & -2 & 0 & 1 \\ 0 & 3 & 0 & 2 & 0 \\ -1 & 0 & 2 & 0 & 3 \end{vmatrix}, \quad \begin{vmatrix} 85 & 17 & 34 & -68 \\ 15 & -5 & 0 & 5 \\ -7 & -14 & 0 & 7 \\ -13 & 13 & 0 & 65 \end{vmatrix},$$

Exercise 3 (4 points)**.**
Explain why the following is true:

$$2^{26} = (((2^2)^2)^2)^2 \cdot ((2^2)^2)^2 \cdot 2^2 = (2 \cdot ((2 \cdot 2^2)^2)^2)^2$$

Compute 2^{26} and 5^{13}.
Remark: The same principle applies when computing powers of square matrices or within finite fields.

Exercise 4 (4 points)**.**
Gaussian elimination can be conducted over any field completely analogously as in the case of real numbers: all operations are performed in the same manner as for real numbers except that all arithmetic operations are arithmetic operations in a field.

(1) Bring the following system of linear equations over the finite field $\mathbb{F}_2$ into triangular form:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

(2) Compute the solution $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4$ of the system of linear system of equations.
(3) Briefly explain why Type II row operations are not very interesting in the special case of Gaussian elimination over $\mathbb{F}_2$.

Bonus Exercise (Diffie-Hellman-Merkle Key Exchange, 2+2+0)**.**
The basic problem of cryptography is the following: Alice and Bob want to communicate over a public channel such that an eavesdropper cannot understand their communication. For that reason, they encrypt their messages before sending and decrypt their messages after receiving. This encryption and decryption depends on an cryptography method that is publicly known and a secret cryptographic key (which is just a number), that is only known to Alice and Bob. Without knowing the secret, an eavesdropper cannot efficiently decipher the encrypted communication.

This requires, however, that Alice and Bob agree on a shared secret in the first place. In many situations, they can only do so via public communication. Paradoxically, even through a public communication channel they can still agree on a shared secret number that is difficult to guess for any eavesdropper.

An algorithm for that purpose is known as the *Diffie-Hellman-Merkle Key Exchange*. It involves computation over finite fields $\mathbb{F}_p$, for which we first review some facts. Let $p \in \mathbb{N}$ be a prime number and let $g \in \mathbb{F}_p$ be an element of the finite field $\mathbb{F}_p$. When $k \in \mathbb{N}$, then the k-th power of g is written g^k and defined in the usual manner: $g^1 = g$, $g^2 = g \cdot g$, $g^3 = g \cdot g \cdot g$, and so on, where all multiplications are computed within $\mathbb{F}_p$. Of course, the typical laws of arithmetics hold: when $k, l \in \mathbb{N}$, then $g^k \cdot g^l = g^{kl}$ and $(g^k)^l = g^{kl}$. Since $\mathbb{F}_p$ has only p elements, the values $g, g^2, \ldots, g^p \in \mathbb{F}_p$ already give all possible powers of g.

The Diffie-Hellman-Merkle Key Exchange between Alice and Bob works as follows.

(i) **Public:** Alice and Bob agree publicly on prime number p and on $g \in \mathbb{F}_p$.
(ii) **Private:** Alice picks $a \in \{1, \ldots, p\}$ and computes $A = g^a$ in $\mathbb{F}_p$.
(iii) **Private:** Bob picks $b \in \{1, \ldots, p\}$ and computes $B = g^b$ in $\mathbb{F}_p$.
(iv) **Public:** Alice sends her result A to Bob, and Bob send his result B to Alice.
(v) **Private:** Alice computes $A' = B^a$ in $\mathbb{F}_p$.
(vi) **Private:** Bob computes $B' = A^b$ in $\mathbb{F}_p$.

One can show (as you do in this exercise) that $A' = B'$, which is the secret number that Alice and Bob agree upon. The secret values a and b are only know to Alice and Bob, respectively, and are never shared directly.

The motivation for the Diffie-Hellman-Merkle Key Exchange is the following: given $g \in \mathbb{F}_p$ and $k \in \mathbb{N}$, it is quite easy to compute $c = g^k$, as you have seen in Exercise 3 above. However, when p is a very large prime number, then it is very difficult to compute the exponent k from the base g and the power c. Essentially, one cannot do much better than simply computing $g, g^2, g^3, \ldots$ until we hit c. This is known as *discrete logarithm problem*. When p is a very large prime number, then the discrete logarithm problem is considered infeasible for practical purposes.

Alice and Bob's public communication involves the prime number p, the base g, and the two intermediate values A and B. But it is difficult to compute the shared secret number C from A and B alone. An eavesdropper would like to compute the exponents a and b used by Alice and Bob, but as mentioned above, this is practically very difficult. Hence, by all practical means, the shared secret number is only known to Alice and Bob.

For practical purposes, p is typically chosen as a very large prime number, and g is a so-called *primitive root modulo p*, which means that the powers $g, g^2, g^3, \ldots$ cover all of $\mathbb{F}_p$. For example, 5 is a primitive root modulo 23, and 20 is a primitive root module 37. But 2 is *not* a primitive root modulo 7.

Complete the following exercises:

(1) Explain why the number A' computed by Alice and the number B' computed by Bob are the same, i.e., $A' = B'$.
(2) Suppose that Alice and Bob have agreed on $p = 23$ and $g = 5$ (which is a primitive root modulo 23). Compute the Diffie-Hellman-Merkle Key Exchange with these parameters, assuming that Alice picks her secret number $a = 4$ and Bob picks his secret number $b = 3$. Verify that their shared secret is $18 \in \mathbb{F}_{23}$. Show the computations.
(3) Pick a friend and share a secret! Perform the Diffie-Hellman-Merkle Key Exchange with the prime number $p = 37$ and $g = 20$.

More information: `https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange`