# Домашна работа №2 - Компютърна алгебра
## Компютърни науки, I курс, 2016/2017г.

Решете задачите с помощта на Maxima или Mathematica. Числата $\alpha, \beta$ и $\gamma$ са последните три цифри на факултетния ви номер.

Задача 1. (1 т.) Дефинирайте списък $L$ с дължина 5, който съдържа цифрите на факултетния ви номер. Изведете всички пермутации на $L$, в които $\gamma$ е на първа позиция.

Задача 2. (2 т.) Дефинирайте множество $S$, което съдържа цифрите на факултетния ви номер и квадратите им.

а) Изведете всички 3-елементни подмножества на $S$, които съдържат числото $\beta$.

б) Съставете списък от произведенията на всички двойки различни числа от множеството $S$.

Задача 3. (2 т.) Дадени са полиномите

$$p(x) = 2x^3 - \beta x^2 + 2\alpha x^2 - \alpha\beta x + 2\beta x - \beta^2;$$

$$q(x) = 3x^4 + 3\alpha x^3 + \gamma x^2 + 3\beta x^2 + \alpha\gamma x + \beta\gamma.$$

а) Намерете най-големия им общ делител $d(x)$, както и частните $\frac{p(x)}{d(x)}$ и $\frac{q(x)}{d(x)}$.

б) Представете ги като списък от коефициенти и намерете сумата им.

Задача 4. (3 т.) RSA

RSA е асиметричен алгоритъм за шифриране на данни, т.е. използва двойка различни ключове при шифриране и дешифриране. Наименованието идва от фамилните имена на създателите му - Ronald Rivest, Adi Shamir И Leonard Adleman. Алгоритъмът на RSA предоставя процедура за подписване на електронен документ и за проверка на автентичността на подписа. RSA е приложен в операционни системи на Майкрософт, Епъл, Сън и Новел. В практиката RSA може да бъде открит в телефони, на мрежови карти за Интернет, на смарт карти и др.

### Генериране на двойка ключове

1. Избират се две различни прости числа $p$ и $q$. За по-добра сигурност те трябва да бъдат случайни и с еднакъв брой цифри (представени в двоична бройна система).
2. Изчислява се $n = pq$. Това е модулът на частния и публичния ключ.
3. Изчислява се функцията на Ойлер: $\varphi(n) = (p-1)(q-1)$.
4. Избира се цяло число $e$, така че $1 < e < \varphi(n)$, и освен това $e$ и $\varphi(n)$ да нямат общи делители. Експонента на публичния ключ е $e$.

5. Изчислява се $d, 1 < d < \varphi(n)$, което удовлетворява уравнението $de \equiv 1(mod\varphi(n))$. С други думи, $ed$–1 се дели без остатък на $(p-1)(q-1)$. Експонента на частния ключ е $d$.

Публичният ключ е съставен от модула $n$ и от публичната експонента $e$ - $(n, e)$. Частният ключ съдържа модула $n$ и частната експонента $d$ - (n,d).

## Шифриране

Получателят предава публичния си ключ $(n, e)$ на изпращача и съхранява частния ключ. Изпращачът изпраща съобщение $M$.

Първоначално $M$ е превърнато в число $0 < m < n$ като се използва предварително договорен за целта протокол. След което се шифрира - изчислява се шифрограмата $c$, където:

$$c \equiv m^e \pmod{n}.$$

## Дешифриране

Получателят възстановява $m$ от $c$, като използва ключовата експонента $d$ от:

$$m \equiv c^d \pmod{n}.$$

Ако е дадено $m$, оригиналното съобщение $M$ може да бъде възстановено, като се обърне схемата.

Доказателство:

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}.$$

Тъй като $ed = 1 + k\varphi(n)$,

$$m^{ed} \equiv m^{1+k\varphi(n)} \equiv m(m^k)^{\varphi(n)} \equiv m \pmod{n}.$$

Последното съждение следва от Теорема на Ойлер, когато $m$ е взаимно просто с $n$. Чрез използване на китайската теорема за остатъците може да бъде доказано, че сравнението важи за всички $m$.

С това се доказва, че сме получили първоначалното съобщение:

$$c^d \equiv m \pmod{n}.$$

## Задача:

Създайте двойка частен и публичен ключ за шифър RSA - $(n, d)$, $(n, e)$, като:

- $p$ е най-голямото просто число, което дели факултетния ви номер.
- $q$ е най-малкото просто число, по-голямо от факултетния ви номер.

- $e$ е най-голямото число, взаимно просто с $\varphi(n)$, ненадвишаващо факултетния ви номер.

С получения частен ключ шифрирайте фамилното си име, като представите буквите му с поредните им номера в кирилицата.

Забележка: Решените задачи трябва да бъдат предадени на един или няколко изпълними файла с разширения $.wxm, .wxmx$(за Maxima) или $.nb$ (за Mathematica). Имената на файловете трябва да съдържат факултетен номер и номер на задача (ако задачите са на отделни файлове).