Tematika, Diszkrét matematika, 2023 őszi félév

Python:

1. A program felépítése, szerkesztése, szerkezete, fordítása, futtatása, megjegyzések használata
2. Típusok, típuskonverziók: **int, float, bool, str, complex, bytes, Decimal, Fraction**
3. Változók: kezdeti értékadás, értékmódosítás: **=, +=, *=, -=,** stb.
4. Egyszerű adatszerkezetek és a velük kapcsolatos műveletek: **list, tuple, bytes**
5. Aritmetikai operátorok: **+, -, *, /, //, %, ****
6. Relációs operátorok: **<, >, ==, !=, <=, >=**
7. Logikai operátorok: **and, or, not**
8. Az **if, while, for** szerkezetek
9. A **range** függvény, az **in** operátor
10. Írás képernyőre, olvasás billentyűzetről: **print, input**
11. Függvények: definiálás, meghívás, paraméterezés, paraméterátadás, rekurzió
12. Állománykezelés (szöveg, bináris): **open, close, write, read, readline, readlines, print**
13. Bitoperátorok: **&, |, ~, ^, >>, <<**
14. Kivételkezelés: **try … except**
15. Könyvtárcsomagok: **math, decimal, fractions, random, base64, time**
16. Könyvtárfüggvények, metódusok: **type, len, sqrt, factorial, pow, log, gcd, ceil, floor, getcontext, radians, chr, ord, index, hex, bin, format, encode, decode, split, strip, randint, getrandbits, b64encode, b64decode, time, bit_length, to_bytes, from_bytes, stb.**

Diszkrét matematika:

1. Természetes számok: keresés, válogatás, faktoriális számolás, számjegyek száma, gyorshatványozás, a legnagyobb közös osztó
2. Szövegállományok adatainak feldolgozása
3. Racionális számok: irreducibilis alak, a racionális számok sorba rendezése, műveletek racionális számokkal, egy racionális szám lánctört jegyei, Farey sorozat
4. Irracionális, valós számok: *híresebb* irracionális számok számjegyeinek kigenerálása, négyzetgyök, k-gyök, logaritmus, polinom helyettesítési értéke
5. Komplex számok: műveletek komplex számokkal, egy másodfokú egyenlet komplex gyökei
6. Számrendszerek: átalakítások, 2^n típusú számrendszerek és a köztük levő kapcsolat
7. Vegyes alapú számrendszerek: faktoriális számrendszer, Fibonacci számrendszer
8. Az n-ik Fibonacci szám
9. Bitműveletek, műveletek 2-vel, 2^k-val, Hamming súly, titkosítás XOR művelettel
10. Bináris állományok hexa, oktális, bináris alakja
11. Kódolási technikák: ASCII, Unicode szabvány
12. Bájtsorrend, utf-8 kódolás
13. Prímszámok, triviális prímtesztelő algoritmusok: osztási próba, Eratoszthenész szitája
14. A számelmélet alaptétele
15. A prímszámtétel, ikerprímek, a Goldhach-sejtés, a Wilson tétel
16. Kongruenciák, maradékosztályok, maradékrendszerek
17. Moduláris hatványozás
18. A kis Fermat tétel, az Euler függvény, az Euler tétel, összefüggések

19. Nem elemi prímtesztelő algoritmus: a Miller Rabin prímteszt
20. Hatványértékek és generátor elemek, biztonságos prímek
21. A diszkrét logaritmus probléma, a brute-force algoritmus, a Diffie-Hellman kulcscsere
22. Az euklideszi algoritmus, a kiterjesztett euklideszi algoritmus
23. Lineáris kongruenciák, moduláris inverz
24. Az RSA-textbook: kulcs generálás, titkosítás, digitális aláírás
25. A kínai maradéktétel és alkalmazásai

Nem kellenek a vizsgára:

- 4. labor, 6. feladat,
- 6. labor, 13 feladat,
- 8 labor, II. feladat,
- 9. labor, II. feladat,
- 11 labor,
- 12 labor.