NÉV: NEPTUN:

ELTE IK Diszkrét modellek alkalmazásai (BSc, 18, F) minta feladatsor

2. zárthelyi dolgozat

A ZH megoldásban kérjük kommentként a bemásolt külső (nem az oktató által kiadott) tartalmak URL-jét feltüntetni. Bármilyen módon generált kód felhasználása tilos.

I. rész (elméleti feladatok)

1. feladat 10 pont

Számolja ki az (a) 5 (b) 7 multiplikatív inverzeit modulo 10-ben.
Döntse el, hogy igazak-e a következő állítások, és indokolja röviden.

(c) A Shamir-titokmegosztásban a polinom szabad tagján kívüli együtthatóinak kisebbnek kell lenniük, mint a titok.
(d) Modulo p prímszám számolva minden nemnulla elemnek létezik multiplikatív inverze.
(e) 10 modulo 7 egyenlő 3 modulo 7-tel.

II. rész (programozási feladatok)

2. feladat 6 pont

Írjon $foo(poly, L)$ szignatúrával függvényt, amely paraméterként fogad *poly* egész együtthatós polinomot ill. L egészek listáját. A függvény térjen vissza azon L-beli egészekkel, amelyek gyökei *poly*-nak. Mutassa be a függvény működését egy példán.

3. feladat 10 pont

A "hello world" sztring titokmegosztásához használja a $100x^{100} + 99x^{99} + ... + x$ polinomot (az együttható és a kitevő 100-tól 1-ig fut), állítson elő 200 db. titokrészletet. Legalább hány ember szükséges az eredeti titok előállításához? Mutassa be, hogy ennyi titokrészletből előállítható az eredeti sztring, azonban 1-gyel kevesebből nem!

4. feladat 14 pont

Írjon
$SSS\_create\_secret\_pieces(required\_num\_of\_people, num\_of\_people, secret, first\_component\_list)$
szignatúrával függvényt, amely a szokásos titokmegosztás paramétereket fogadja, valamint egy $first\_component\_list$ paramétert, amely sztringek listája. A függvény feladata, hogy titokrészleteket állítson elő a *secret* titokhoz, de úgy, hogy a hívó meg tudja mondani, mi legyen a titokrészletek első komponense. Amennyiben a $first\_component\_list$ lista hossza nem egyezik meg num_of_people-al, a függvény dobjon $ValueError$ kivételt. A függvény készítsen titokrészleteket, ahol az egyes titokrészletek első komponense a $first\_component\_list$ megfelelő eleme, a második komponens pedig az adott sztring számbeli reprezentációjához rendelt polinom helyettesítési érték. A megoldáshoz felhasználhatja az órai programozási feladatok függvényeit, vagy teljesen újat is készíthet.

A függvénnyel készítsen 5 db. titokrészletet a "DiModAlk" sztringhez, ahol legalább 3 ember legyen szükséges az eredeti sztring előállításához, a titokrészletek első komponensei pedig: "CCC", "cpp", "CRC", "ETC", "AS". Mutassa be, hogy a generált titokrészletekből előállítható az eredeti sztring.

Koch-Gömöri Richárd, kgomoririchard@inf.elte.hu, kgomori.richard@gmail.com