Bevezetés a számításelméletbe II.

14. gyakorlat, 2014. május 13.

Tudnivalók

Fermat-teszt Adott n számról kell eldönteni, prím-e egy véletlen $1 < k < n$ szám segítségével. Ha $(n,k) > 1$, akkor n nem prím, és k az n *leleplezője*, mert egy osztót is megtudunk a segítségével. Ha $(n,k) = 1$, akkor ha $k^{n-1} \not\equiv 1(n)$, akkor k az n *árulója*, és n bizonyosan nem prím, míg ha $k^{n-1} \equiv 1(n)$, akkor k az n *cinkosa*, és n „valószínűleg" prím.

Állítás Ha n-nek van árulója, akkor az n-hez relatív prím számoknak legalább a fele áruló.

Definíció Az n *Carmichael szám*, ha n összetett, de nincs árulója.

Definíció Az $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ bijekció *egyirányú függvény*, ha f gyorsan számítható, de az f^{-1} kiszámítása pusztán f ismeretében reménytelen. Az f egyirányú függvény *kiskapus egyirányú függvény*, ha létezik f^{-1} kiszámítására is hatékony módszer (amit persze f ismeretében reménytelen megtalálni).

Nyilvános kulcsú titkosírás Egy M üzenetet akarunk kódolni. Feltehető, hogy M egy 0 és n közötti szám, ami az üzenet blokkokra darabolásával elérhető. Értelmes feltevés, hogy az üzenet utolsó néhány betűje véletlen karakterekből áll. A címzettnek közzétette az f kiskapus egyirányú függvényét, amit bárki könnyen kiszámíthat. Az f^{-1} hatékony kiszámítására csak a címzett képes. Az M üzenet helyett az $X = f(M)$-t küldjük el, mert ebből egyedül a címzett képes kiszámítani $f^{-1}(X) = f^{-1}(f(M)) = M$ üzenetet.

Digitális aláírás Az A játékos szeretne B-nek egy M üzenetet úgy elküldeni, hogy B biztos legyen abban, hogy azt A küldte. f_A ill. f_B a nyilvános titkosítófüggvényeik. A az M helyett $f_B(f^{-1}(M))$-t küldi. Ebből csak B képes M-t megfejteni, és mások számára is bizonyítani tudja, hogy azt A aláírta.

Az RSA eljárás Legyenek p, q prímek, $n = pq$, $m = \varphi(n) = (p-1)(q-1)$. Legyen $e > 1$ olyan, amire $(e,m) = 1$, és legyen d $ex \equiv 1(m)$ kongruencia megoldása. A nyilvános kulcs (n,e), a titkos kulcs (n,d). Az f kódolófüggvényt $M \mapsto M^e(\mod n)$, az f^{-1} dekódolófüggvényt pedig $X \mapsto X^d(\mod n)$ írja le.

Feladatok

1. Testet alkot-e a $\{p + q\sqrt[3]{2} : p, q \in Q\}$ halmaz a szokásos szorzásra és összeadásra?

2. Mutassuk meg, hogy ha $a + a = 0$ teljesül a T test valamely $a \neq 0$ elemére, akkor T tetszőleges x elemére $x + x = 0$ teljesül.

3. Határozzuk meg a kvaterniótestben az $x = 2 - j$ ill. az $y = 2 - i + j - k$ elemek inverzeit. Számítsuk ki a $Q(\sqrt{2})$ testben a $(2 + 5\sqrt{2}) \cdot (3 - 2\sqrt{2})^{-1} = \frac{2+5\sqrt{2}}{3-2\sqrt{2}}$ elemet.

4. Bizonyítsuk be, hogy $\{a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} : a, b, c, d \in Q\}$ test és egyúttal 2-dimenziós vektortér a $\{a + b\sqrt{2} : a, b \in Q\}$ test felett!

5. Ha R gyűrű, és $Z \cap R = \emptyset$, akkor gyűrűt alkot e a $\{(r,z) : r \in R, z \in Z\}$ halmaz, ahol $(r,z) + (r',z') := (r + r', z + z')$ illetve $(r,z) \cdot (r',z') := (r \cdot r' + z \cdot r' + z' \cdot r, z \cdot z')$ definiálják a műveleteket, a $nr := r + r + \ldots + r$ $[n]$-szer konvencióval?

6. Határozzuk meg $k \leq n$ esetén az $n! + k$ és $(n+1)! + k$ számok legnagyobb közös osztóját.

7. Igazoljuk, hogy az Euklideszi algoritmusban $2a_{i+2} \leq a_i$.

8. Döntsük el, van-e közös komplex gyöke a $p(x) = 3x^3 - 2x^2 + x - 1$ és a $q(x) = 10x^2 + 101x - 3$ polinomoknak.

9. Mutassuk meg, hogy az 561 Carmichael szám.

10. Az angol ABC betűit a $0, 1, \ldots, 25$ számok kódolják: $A = 0, B = 1, \ldots Z = 25$. Sikerült elfogni az RSA titkosítással kódolt $59, 2, 59, 20, 44, 52$ üzenetet, amit az oktondi feladó betűnként kódolt a címzett $(85, 43)$ nyilvános kulcsával. Törjük fel a kódot, fejtsük meg az üzenetet.

11. Egy lakattal lezárható ládában szeretnénk titkokat küldeni az ismerősünknek. Sajnos azonban a postás minden olyan küldeményt felnyit, amit csak tud, és amit abban talál, azt ellopja vagy lemásolja. Mindkettőnknek van lakatunk, megfelelő kulcsokkal, de egyikünk sem rendelkezik olyan kulccsal, amihez való lakat a másiknál van. Hogyan oldható meg a biztonságos csomagküldés?

12. A és B üzletelnek. A k féle információt árul B-nek, mindegyiket ugyanannyiért. B úgy szeretne vásárolni, hogy A ne tudja meg, mire kíváncsi. Hogyan járhatnak el?