SEMINAR IZ KRIPTOGRAFIJE

RSA (nadaljevanje)

predava:

Miro Masnoglav (MORS)

23. marec 1998

Na zadnjem seminarju:

- Miro Masnoglav:
  Sistem RSA in faktorizacija
  - uvod
  - teorija števil (A.J. o razširjenem Evklidovem algoritmu)
  - kriptosistem RSA
- rešitvi nalog 1.2 (N. Jukić) in 3.2. (J. Blatnik)

Današnji načrt

- Miro Masnoglav (nadaljevanje):
  Sistem RSA in faktorizacija
  - implementacija RSA
  - probabilistično testiranje praštevilčnosti
  - A.J.: Gaussov izrek o kvadratni recipročnosti
  - napadi na RSA
- reševanje nalog 3. poglavja

O sistemu RSA in faktorizaciji bo nadaljeval

Miro Masnoglav (MORS)

Gaussov izrek o kvadratni recipročnosti (1796):

Def. Legendrov simbol

$$\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{če } q \text{ popoln kvadrat mod } p \\ -1, & \text{sicer} \end{cases}$$

Izrek o kvadratni recipročnosti:
Če sta p in q različni lihi praštevili, potem velja

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ter za praštevilo 2:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Zakaj je ta izrek tako pomemben?

Pomaga nam, da odgovorimo kdaj imajo kvadratne kongruence rešitev, saj velja multiplikativno pravilo:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Predstavlja pa tudi nepričakovano zvezo med pari praštevil (globoko pravilo, ki ureja praštevila).

ESIENSTEINOVA LEMMA:
Označimo množico $\{2, 4, 5, \ldots, p-1\}$ z a in naj bo r ostanek (mod p) poljubnega sodega večkratnika qa. Potem je

$$\left(\frac{q}{p}\right) = (-1)^{\sum r}.$$

Dokaz: Če za $a \neq a'$ velja

$$(-1)^{qa} qa \equiv (-1)^{qa'} qa',$$

zaključimo $a = \pm a'$ kar ni mogoče.

Od tod dobimo

$$q^{\frac{p-1}{2}}\prod a \equiv \prod r \pmod p$$

in

$$\prod a \equiv (-1)^{\sum r}\prod r \pmod p.$$

Torej velja: $q^{\frac{p-1}{2}} \equiv (-1)^{\sum r} \pmod p$ in po Eulerjevem kriteriju $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \pmod p$ je dokaz končan. □

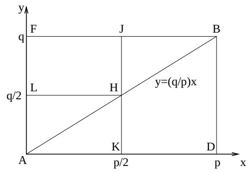
Oglejmo si Eisensteinov dokaz Gaussovega izreka o kvadratni recipročnosti.

Očitno velja:

$$\sum qa = p\sum\left\lfloor\frac{qa}{p}\right\rfloor + \sum r.$$

Ker so elementi a vsi sodi in je p lih, velja $\sum r \equiv \sum\left\lfloor\frac{qa}{p}\right\rfloor$ (mod 2) in zato iz E. leme sledi

$$\left(\frac{q}{p}\right) = (-1)^{\sum\lfloor\frac{qa}{p}\rfloor}.$$



Vsota $\sum\lfloor\frac{qa}{p}\rfloor$ je enaka številu celoštevilčnih točk s sodo x-koordinato v notranjosti trikotnika ABD, ker pa je $q-1$ sod, je ta vsota enaka številu celoštevilčnih točk v notranjosti trikotnika AHK. ... □

Reševanje domačih nalog iz III. poglavja:

Do naslednjega tedna

- preberite 4. poglavje (do str. 155)

nadaljujte z reševanjem nalog 4. poglavja

Stinsonovega učbenika
Cryptography, Theory and Practice

Prihodnjič: Arijana Žitnik konča s 4. pogl.

- Rabinov kriptosistem
- algoritmi za faktorizacijo

Čez 14 dni: A.J. prične s 5. poglavjem

- Drugi javni kriptosistemi
  ElGamalov kriptosistem in diskretni logaritem

Čez 21 dni:
dobrovoljec konča s 5. poglavjem:

- Markle-Hellmanov sistem (nahrbtnik)
- McEliece sistem (error-correcting codes)