ODABRANE TEME IZ TEORIJE BROJEVA: ŠESTA ZADAĆA

1. Sage

a) Implementirajte algoritam koji rješava problem diskretnog logaritma za eliptičke krivulje iz b) zadatka idućeg odjeljka.

2. Eliptičke krivulje nad lokalnim poljima

a) Neka je E/K eliptička krivulja i m prirodan broj relativno prost s $char(k)$. Dokažite da je $E_0(K^{nr})/mE_0(K^{nr}) = 0$. ($K$ je potpuno lokalno polje, K^{nr} maksimalno neramificirajuće proširenje, k rezidualno polje od K, ...)

b) Riješite zadatak 7.13. iz (novog izdanja) Silvermana. (Trebat ćete naučiti nešto o formalnom logaritmu...)

Rok za predaju zadaće je četvrtak 16.2.