ODABRANE TEME IZ TEORIJE BROJEVA: ČETVRTA ZADAĆA

1. Sage

a) Nađite tri proširenja Diofantove trojke $\{1, 8, 120\}$ do racionalne Diofantove četvorke.

b) Provjerite asocijativnost zbrajanje na eliptičkoj krivulji $y^2 = x^3+ax+b$. Možete pretpostaviti da su koordinate svih točaka međusobno različite. (Ovo možete riješiti elegantno u Sage-u tako da konstruirate eliptičku krivulju $y^2 = x^3+ax+b$ nad odgovarajućim funkcijskom poljem s varijablama $a, b, x_1, y_1, x_2, y_2, x_3, y_3$ koje zadovoljavaju relacije $y_i^2 - x_i^3 - ax_i - b = 0$ za $i = 1, 2$ i 3.)

2. Eliptičke krivulje

a) Pročitajte dokaz Teorema 4.2. (2-descent) u Knapp: Elliptic Curves, str. 85.

b) Pročitajte odjeljak 8.(iii) u Cassels: Lectures on Elliptic curves, str. 35-36 pa zapišite eliptičku krivulje $y^2 = x^4 + 1$ u standardnom obliku $y^2 =$ polinom trećeg stupnja. Pomoću Sage-a izračunajte Mordell-Weilovu grupu te krivulje. Koristeći taj rezultat dokažite da jednadžba $x^4 + y^4 = z^2$ nema rješenja u prirodnim brojevima.

Rok za predaju zadaće je četvrtak 12.1.