

楕円曲線上の離散対数問題

p を素数とする. 有限体 $\mathbb{F}_p$ 上の楕円曲線 E の有理点 P, Q が与えられる. $Q = [n]P$ となる n が存在すると仮定する. このとき, $Q = [n]P$ をみたす最小の $n > 0$ を求めよ. (この n のことを $\log_P Q$ と書くこともある.)

10万ドルの懸賞問題 (ECCp-359)

$$p = 815061317237192195822186322581994619328922585201839923945006339195983 \\ 201432548797517008668016697623370770793$$

とおく. p は素数である. $\mathbb{F}_p$ 上の楕円曲線

$$E : y^2 = x^3 + ax + b$$

を考える. ただし,

$$a = 77680889228907375417657860521583838255883364289275509088226901356017 \\ 596063151420052611792807246929378737250$$

$$b = 540052139166202049494615026489876778063087368045457140040430850046014 \\ 315377063270334036826942458933068795336$$

である. E の $\mathbb{F}_p$ -有理点 $P(x_1, y_1)$, $Q(x_2, y_2)$ を考える. ただし,

$$x_1 = 436380050954626345676078162017830257600151100800199888023343691962 \\ 754781525539435543106999289514276178571565$$

$$y_1 = 471243985651744691350627749622973843372651017742187035672634177651 \\ 217385987084628377827075408784363746507946$$

$$x_2 = 154923222221389297989395722093479578520004328910499058567401281708 \\ 520560516387658687672398460070304026697904$$

$$y_2 = 192780495157110678925498883993149085420482196034902970742634047250 \\ 036315574562347482388525311477589535662397$$

である. $Q = [n]P$ となる n が存在することが知られている. $Q = [n]P$ をみたす最小の $n > 0$ を求めよ.

The Certicom ECC Challenge のうち最も難しい問題. この問題の解決には 3.7×10^{45} 日かかると見込まれている. (50 億年 $= 50 \times 365 \times 10^8 = 1,825,000,000,000 \div 1.8 \times 10^{12}$ 日)
離散対数問題の難しさを応用して, 解読しにくい暗号を設計することができる (楕円曲線暗号).