sage: F = FiniteField (0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F)

sage: C = EllipticCurve ([F (0), F (7)])

sage: G = C.lift\_x(0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798)

sage: N = FiniteField (C.order())

sage: P = P=-C.lift\_x(0x11db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5c)

sage: def forge(c, a=-1):

....: a=N(a)

....: R=c\*G+int(a)\*P

....: s = N(int(R.xy()[0]))/a

....: m = N(c)\*N(int(R.xy()[0]))/a

....: print('hash1=',m)

....: print('r1=',int(R.xy()[0]))

....: print('s1=',s)

....:

sage: for c in range(1,10):

....: forge(c)

....:

hash1= 73891928093667100541666205043898441267587758657794766782750716307536286039192

r1= 41900161143649094881904779964789466585249805621280137599854446833981875455145

s1= 73891928093667100541666205043898441267587758657794766782750716307536286039192

hash1= 62205149388825786737310199459980893542365046604564124404118402392687929599561

r1= 26793469924245204343130392774353507155236258837255389989243380374415115947388

s1= 88998619313070991080440592234334400697601305441819514393361782767103045546949

hash1= 71630502409465362978513962569334322089979380375179524546119672056098799075844

r1= 53317892021722342622876002482680497871898582727656761406363551408979174637610

s1= 62474197215593852800694982526007409980938981551418142976241611732538986856727

hash1= 42682765006860785319055238886295612444075886123150037123847753593787330986229

r1= 18277331057613852526128936530598073852190419538981216814689352386932707627027

s1= 97514758179702342897442048478089834000647144740093687567915810754585453867310

hash1= 86485944092969512650498312976117725660492949546578513892865976650129674924118

r1= 75336482571259053808757125411726781150171461513944220727510935183188594210646

s1= 40455606666057141614813859596961126702666102765130683655094227958329567283691

hash1= 17829874277836558369872943186444646293525636979518783068827999188688713653040

r1= 74223080445238037220735166141384497519637436689463472410265442229563988720718

s1= 41569008792078158202835818867303410333200127589611431972339720911954172773619

hash1= 104956150280772071570120927855798599078772297717549559775953988248939923600679

r1= 1547991279506303407635722450412758396295038080217906372378739270368319699094

s1= 114244097957809892015935262558275149456542526198856998010226423871149841795243

hash1= 98693975431246327498391958662908888004484098864570139018514388736027437610628

r1= 45559297689752306774486497671480342925858269781466184813988282978755651045840

s1= 70232791547563888649084487337207564926979294497608719568616880162762510448497

hash1= 25292222169426362969760742810503101183086560848420849767135309758511048414376

r1= 61518691557461623794232686914770715342344584505217074682876722883231084339701

s1= 54273397679854571629338298093917192510492979773857829699728440258287077154636