Code: Iwasawa Invariants and Kida's formula

Debanjana Kundu and Anwesh Ray

February 24, 2022

```
# First we check that E has additive reduction of type I_2* in our \
    field K and that the Tamagawa number at the prime above 2 is not \
    divisible by 5
E = EllipticCurve('32a2'); E
E.local_data()
K.<i> = NumberField(x^2+1)
EK=E.base_extend(K); EK
EK.local_data()
# Next we compute the division field, and this is the calculation \
    that appears in p. 23
L.<b> = E.division_field(5); L
```

```
Elliptic Curve defined by y^2 = x^3 - x over Rational Field
[Local data at Principal ideal (2) of Integer Ring:
Reduction type: bad additive
Local minimal model: Elliptic Curve defined by y^2 = x^3 - x over Rational Field
Minimal discriminant valuation: 6
Conductor exponent: 5
Kodaira Symbol: III
Tamagawa Number: 2]
Elliptic Curve defined by y^2 = x^3 + (-1)*x over Number Field in i with defining
polynomial x^2 + 1
[Local data at Fractional ideal (i + 1):
Reduction type: bad additive
Local minimal model: Elliptic Curve defined by y^2 = x^3 + (-1)*x over Number Field in i
with defining polynomial x^2 + 1
Minimal discriminant valuation: 12
Conductor exponent: 6
Kodaira Symbol: I2*
Tamagawa Number: 4]

Number Field in b with defining polynomial x^32 - 40*x^31 + 12000*x^29 - 10760*x^28 -
266800*x^27 + 11468000*x^26 - 1096600000*x^25 - 5566913400*x^24 + 142092440000*x^23 +
4369939320000*x^22 - 378135400000*x^21 - 257156918536000*x^20 - 6566363103320000*x^19 -
68617519071000000*x^18 + 71545316608000000*x^17 + 1021924638742710000*x^16 +
12076511879430640000*x^15 + 119254107475077600000*x^14 + 1195746480884630000000*x^13 +
```

82847553195104300000000*x^12 + 126553853881640250000000*x^11 +
17074052628101627500000000*x^10 + 17231192395388340000000000*x^9 +
14554413324934569062500000000*x^8 + 9447284167114381875000000000*x^7 +
4931812499156815000000000000*x^6 + 1290930974132151562500000000000*x^5 -
235024652475789062500000000*x^4 - 68231143169029687500000000000*x^3 -
4757864118392539062500000000000*x^2 + 24627499323070312500000000000000*x +
145042690557131347656250000000

```
# The modular polynomial is obtained from Sutherland's Website. We \
   use this to find primes that are split in the 5-division field. \
   This explains the calculations stated on p.24.
E=EllipticCurve('32a2');E
P = Primes()
q=1
for p in range(1,10000000):
    if p in P:
        if p%20==1:
            ap=E.ap(p)
            if ap%5==2:
                F.<a> = GF(p)
                R.<x> = PolynomialRing(F)
                f=14135994715472135869775347469107136275100467200+ \
   532743308034244254504201602733565091512320000*x- \
   (26407345707662059625971579024797878294937 6*1728)*x+  \
   669250004262799770848714941501506846720 0*x\
   ^2+(365547365839496292957064723326566400 00*1728)*x^2 \
   +(51109417775524180831107651993600000*1728^2)*x\
   ^2+28024477782843952780432156529786880 0*x\
   ^3-(19245793461892829965510823116800 0*1728)*x^3+ \
   (26898488858380731577417728000*1728^2)*x\
   ^3-(44120696551291483524610 0*1728^3)*x\
   ^3+12847331328414244562534 40*x^4+ 12854179890682881638400 0*1728*x\
   ^4+ (3830836097798112153 75*1728^2)*x^4+  \
   (107878928185336800*1728^3)*x^4+ (1665999364600 *1728^4)*x^4 + \
   1963211489280*x^5- (246683410950 *1728)*x^5 + (2028551200 \
   *1728^2)*x^5-  (4550940*1728^3)*x^5+  (3720 *1728^4)*x^5-1728^5*x\
   ^5+ x^6
                g=f.factor()
                if len(g)==6:
                    p
                    g
                    q=q*p
```

Elliptic Curve defined by y^2 = x^3 - x over Rational Field

63241

(x + 9130) * (x + 26600) * (x + 28822) * (x + 31643) * (x + 37410) * (x + 60303)
63901
(x + 15646) * (x + 16523) * (x + 16743) * (x + 31583) * (x + 36229) * (x + 58255)
514561
(x + 17980) * (x + 101289) * (x + 151599) * (x + 182445) * (x + 373335) * (x + 408026)
1311341
(x + 52741) * (x + 110805) * (x + 329163) * (x + 468361) * (x + 847253) * (x + 994290)
2399081
(x + 86400) * (x + 504130) * (x + 586282) * (x + 628249) * (x + 1659414) * (x + 1969971)
2502301
(x + 849060) * (x + 975367) * (x + 986711) * (x + 992264) * (x + 1695383) * (x + 2202878)
2620301
(x + 254240) * (x + 616970) * (x + 841661) * (x + 953604) * (x + 1923419) * (x + 2213531)
2790461
(x + 102295) * (x + 192494) * (x + 1355869) * (x + 1518982) * (x + 2305491) * (x +
2307028)
3325121
(x + 50010) * (x + 962791) * (x + 1675863) * (x + 2715705) * (x + 2842069) * (x + 3279506)
3436501
(x + 498157) * (x + 1240968) * (x + 1806448) * (x + 3046317) * (x + 3296212) * (x +
3378228)
4046401
(x + 296622) * (x + 1042510) * (x + 1698426) * (x + 2679209) * (x + 3037843) * (x +
3347435)
4050281
(x + 321598) * (x + 341653) * (x + 1735296) * (x + 1766755) * (x + 2454308) * (x +
2750706)
4559101
(x + 317131) * (x + 2229535) * (x + 2688638) * (x + 3136401) * (x + 4533261) * (x +
4548759)
4800421
(x + 762946) * (x + 2042769) * (x + 2522505) * (x + 4450345) * (x + 4626595) * (x +
4721505)
5403361
(x + 1878513) * (x + 1925695) * (x + 2143400) * (x + 2707567) * (x + 3612058) * (x +
5056061)
5609321
(x + 84459) * (x + 1437083) * (x + 1931703) * (x + 3183001) * (x + 3524645) * (x +
4755308)
6660221
(x + 8744) * (x + 636210) * (x + 2105557) * (x + 2334949) * (x + 4790581) * (x + 5541667)
7601861
(x + 2449981) * (x + 2503227) * (x + 2965639) * (x + 3111788) * (x + 5621555) * (x +
6265345)
7959521
(x + 1420617) * (x + 2291447) * (x + 4807537) * (x + 5834593) * (x + 6036006) * (x +
7164412)

8942501
(x + 239420) * (x + 328509) * (x + 2709441) * (x + 4344275) * (x + 7514816) * (x + 8792286)
8959921
(x + 2613178) * (x + 2873789) * (x + 4884804) * (x + 7029077) * (x + 7236754) * (x + 8450500)
9181901
(x + 1847350) * (x + 2851740) * (x + 3685566) * (x + 3936128) * (x + 6923677) * (x + 7148427)
9187081
(x + 315782) * (x + 4246488) * (x + 5028613) * (x + 6825597) * (x + 8131514) * (x + 8346407)
9437321
(x + 937281) * (x + 1554383) * (x + 3490567) * (x + 3940138) * (x + 5864917) * (x + 6568184)

```
# We need to find a value of t such that E_t has bad reduction at \
    the two primes 63241 and 63901. We find values of n such that f(n\
    ) is divisible by the prime in question. Then, we shall use the \
    Chinese remainder theorem to find a value of t in the next step.
q=63241
for n in range(0,q):
    a=125*n^12 - 550*n^10 - 825*n^8 + 220*n^6 - 165*n^4 - 22*n^2 + 1
    if a%q==0:
        if a%q^2!=0:
            n
```

5364
8824
17137
18473
19497
24186
39055
43744
44768
46104
54417
57877

```
q=63901
for n in range(0,q):
    a=125*n^12 - 550*n^10 - 825*n^8 + 220*n^6 - 165*n^4 - 22*n^2 + 1
    if a%q==0:
        if a%q^2!=0:
            n
```

2597
12556

```
14731
15634
23918
30114
33787
39983
48267
49170
51345
61304
```

```
# We need to find a value which is 5364 mod 63241 and 2597 mod \
    63901. Then, f(t) is divisible by the primes 63241 and 63901 \
    exactly once.
1059545078%63241==5364
1059545078%63901==2597
```
```
True
True
```

```
n=1059545078
m=125*n^12 - 550*n^10 - 825*n^8 + 220*n^6 - 165*n^4 - 22*n^2 + 1
m
factor(m)
```
```
250232245585268125419538458509590060143570955451160586952870836011406272257508347893645190
780082524494395578393
13 * 401 * 63241 * 63901 * 21068381440942021 * 23007701426021875081 *
245044387414758252043049981735164067194758331434782579693662 21
```

```
# Finally we need to check that the curve E_2 satisfies our \
    assumptions. This computation is used in the proof of Lemma 7.4.
E = EllipticCurve\
    ([0,168296446137189087194501767921833910783492001998159631069715319976183253

E
K.<i> = NumberField(x^2+1)
EK=E.base_extend(K)
pp = K.fractional_ideal(1+i)
da = EK.local_data(pp)
da
D=E.discriminant()
d=D/64
d/245044387414758252043049981735164067194758331434782579693662 21
```
```
Elliptic Curve defined by y^2 = x^3 +
```

16829644613718908719450176792183391078349200199815963106971531997618325346518195 30*x^2 -
9
93662245131229552648588593285186674586767625060731750375440560448499460404026226591487189176367949528696260899356431612520935180977428921937667494177305190605344105132321810564462430 1*x - 27927380694219820819116212863062552373448346890426050059883907340261159020802156537659423817307702684434715856769478961661097274943038438846454560306253652897975342455422559865683172423679026646781904599620497538386099333960907529891138922491778688076124984996982980 14 over Rational Field
Local data at Fractional ideal (i + 1):
Reduction type: bad additive
Local minimal model: Elliptic Curve defined by y^2 = x^3 + (-9936622451312295526486830055977947005455291529347623620918881639808601361128824425275182468380619604870552623713475925481906076327138018564172291638345667267344897299631900352207764601)*x + (-27871637419381058701212836002757783524416058628731637202157563713726615433635933678319769790710964169087272719749176248935121961602087197717484592245944105855836187191728295168857693952996052752556324497429724398705489226785334580718389523417260718790020501511914596504) over Number Field in i with defining polynomial x^2 + 1
Minimal discriminant valuation: 12
Conductor exponent: 6
Kodaira Symbol: I2*
Tamagawa Number: 4
40037929151747746598527347460611880840856520746128709292210331064568578702445674883936634168571200467311236207656044136256999039130622789748907305402199239393807692080617980410866906896143988242091016908068436249089835798519655704240307575343275363512650320397122244905168933956185026725349580188784969160696823605766548111822413031971805680239077394971419273506169081597917091869693826062506011015490841930027001913944245769194021359583445932061338902130463539390819468083288157818107571933