ass7ecDRAFT

Name(s):

```
# Matteo Durante
```

```
# Waifod
```

Elliptic curves

Mastermath, The Netherlands, Spring 2019

This worksheet introduces you to some basic things you can do with elliptic curves in SageMath. It includes several exercises, for which you might want to open a new worksheet to experiment in with all kinds of functions. For those taking the class for credit, all these exercises are homework.

Some rules regarding the homework:

- Include in this worksheet an explanation of what you did to solve the exercises. This will sometimes consist of a short proof instead of a list of commands (which you could include in a cell as comments using a #-sign).
- Homework needs to be handed in as PDF or printed on paper, make sure the output is visible on the paper or PDF!
- To enable the assistant to verify your computations, you must share your SageMath worksheet (see below for the ways in which you can do this).
- Homework can be handed in in groups of 2.
- We do not make backups of the content of the server, so make sure to make your own backups, for example by clicking "File..." and then "Save worksheet to a file...", or by clicking "Edit" and then copying the content to an email.
- When working together, do **not** use only one account to log in on two computers at the same time. Use one account on one computer, or two accounts on two computers.

Help with SageMath in general is available through http://www.sagemath.org/ and in particular the tutorial at http://www.sagemath.org/doc/tutorial/ is very useful for beginners. Information about elliptic curves in particular is on http://doc.sagemath.org/html/en/reference/curves/index.html#elliptic-curves.

Construction of elliptic curves and points (exercise 1)
Number of points of the reduction and torsion (exercise 2,3,4,5)
Bad reduction (exercise 6,7,8,9)

The Frobenius endomorphism (exercise 10, 11, 12)
Mordell-Weil groups (exercise 13,14)
Period lattices (exercise 15,16)
Diophantine equations (exercises 17 and 18)
Modularity (exercise 19)
Heights (exercise 20)

Write here in which way you provide your worksheet electronically to the assistant:

1) using the "Share" button on sage.math.leidenuniv.nl and sharing with the assistants' usernames (which we will add to the web page later)

2) downloading the .sws file and uploading it together with the pdf on the webpage of Mastermath

3) sharing your worksheet with the assistants on CoCalc (again: we will add their usernames to the web page later).

One way to specify an elliptic curve is by a pair $[a,b]$ of coefficients in the Weierstrass equation $y^2 = x^3 + ax + b$.

```
a = -43
b = 166
E1 = EllipticCurve([a,b])
E1
```

```
Elliptic Curve defined by y^2 = x^3 - 43*x + 166 over Rational Field
```

Verify that the discriminant of E_1 agrees with the definition from the lectures.

```
D1 = E1.discriminant()
D1 == -16*(4*a^3+27*b^2)
```

```
True
```

Recall that <tab> after 'E1.' shows everything you can do with E_1. Then compute the j-invariant of E_1.

```
E1.
```

```
Traceback (click to the left of this block for traceback)
...
SyntaxError: invalid syntax
```

A point is defined by coercing a list of two affine or three homogeneous coordinates into E_1.

```
P = E1([3,8])
P
```

```
(3 : 8 : 1)
```

Exercise 1: Compute nP for all integers n.

Answer:

P.order() returns the order of the point P, range(n) gives the list of integers from 0 to n-1.

Given any n, nP is given by the i-th element of the following list, where i=n mod 7 with 7 being the order of P.

```
print "The order of the torsion point P is:", P.order()
[(n,n*P) for n in range(P.order())]
```

```
The order of the torsion point P is: 7
[(0, (0 : 1 : 0)),
 (1, (3 : 8 : 1)),
 (2, (-5 : -16 : 1)),
 (3, (11 : -32 : 1)),
 (4, (11 : 32 : 1)),
 (5, (-5 : 16 : 1)),
 (6, (3 : -8 : 1))]
```

Back to top

With E.Np(r) we get the number of points on the reduction of E to the finite field of r elements, where r is prime (including the singular point, if it exists).

Exercise 2: Create a list of the number of $\mathbb{F}_p$-points on the reduction of E_1 modulo p for all primes p of good reduction under 100.

Answer:

```
[(p, E1.Np(p)) for p in primes(100) if gcd(p, D1)==1]
```

```
[(3, 7),
 (5, 7),
 (7, 7),
 (11, 14),
 (17, 21),
 (19, 14),
 (23, 28),
 (29, 28),
 (31, 28),
 (37, 35),
 (41, 42),
 (43, 49),
 (47, 35),
 (53, 42),
 (59, 70),
 (61, 70),
 (67, 70),
 (71, 77),
 (73, 84),
 (79, 84),
 (83, 84),
 (89, 84),
 (97, 84)]
```

Exercise 3: What is the greatest common divisor of those numbers and what does this say about the torsion subgroup of $E_1(\mathbb{Q})$?

Answer:

```
list = [E1.Np(p) for p in primes(100) if gcd(p, D1)==1]
print "The required gcd is:", gcd(list)
```

```
The required gcd is: 7
```

We see that $|E_1(\mathbb{F}_p)| = 7$ for $p = 3, 5$. Also, for any n s.t. $p \mid n$ we have an injection $E_1(\mathbb{Q})[n] \to E_1(\mathbb{F}_p)$, hence the cardinality of $E_1^{tors}(\mathbb{Q})$ has to divide both $3^a \cdot 7$ and $5^b \cdot 7$. It follows that it has to divide 7. On the other hand, we know that the earlier described point P is torsion and it has order 7, thus $|E_1^{tors}(\mathbb{Q})| = 7$.

Exercise 4: Find a function that computes the size of the torsion group and verify your answer to the previous exercise.

Answer

```
E1.torsion_order()
```

```
7
```

Note that you can also define an elliptic curve by its Weierstrass equation after declaring x and y as variables.

```
x,y = var('x,y')
C = EllipticCurve(y^2 + x*y -5*y == x^3 - 5*x^2)
C
```

```
Elliptic Curve defined by y^2 + x*y - 5*y = x^3 - 5*x^2 over
Rational Field
```

Exercise 5: Compute the torsion subgroup of the elliptic curve given by $y^2 + xy - 5y = x^3 - 5x^2$.

Answer:

```
x,y = var('x,y')
C = EllipticCurve(y^2 + x*y -5*y == x^3 - 5*x^2)
C.torsion_subgroup()
```

```
Torsion Subgroup isomorphic to Z/4 + Z/2 associated to the Elliptic
Curve defined by y^2 + x*y - 5*y = x^3 - 5*x^2 over Rational Field
```

Back to top

Bad reduction

We can also define an elliptic curve E_2 by specifying the coefficients a_1, a_2, a_3, a_4, a_6 of a long Weierstrass equation.

```
a1=0
a2=0
a3=1
a4=9
a6=0
E2=EllipticCurve(QQ,[a1,a2,a3,a4,a6])
E2
```

```
Elliptic Curve defined by y^2 + y = x^3 + 9*x over Rational Field
```

Exercise 6: Compute the discriminant of E_2 and factorize it.

Answer:

```
D2 = E2.discriminant()
print "The discriminant of E2 is:", D2;
print "Its factorization is:", D2.factor()
```

```
The discriminant of E2 is: -46683
Its factorization is: -1 * 3^3 * 7 * 13 * 19
```

From the (correct) answer to the previous exercise, we see that the only primes of bad reduction are $3, 7, 13$, and 19.

Exercise 7: Compute for each prime of bad reduction of E_2 the number of points on the reduction.

Answer:

```
[(p, E2.Np(p)) for p in [3,7,13,19]]
```

```
[(3, 4), (7, 9), (13, 15), (19, 19)]
```

Recall from the lectures that the nonsingular points on a singular Weierstrass curve over a field k are in bijection with the elements of one of three groups, namely k (additive, when the singular point is a cusp), or k^* (split multiplicative, for a node with tangents defined over k), or the kernel of the norm from l^* to k^* where l is a quadratic field extension of k (nonsplit multiplicative, for a node whose tangents are defined over l).

Exercise 8: Use the number of points counted above to read off the types of singular reduction (additive, split multiplicative or nonsplit multiplicative) of E_2 at its primes of bad reduction.

Answer: (just text, so no sage-commands

We see that, for p=3, we have 3 non-singular points, hence the group is isomorphic to Z/3Z. The singular reduction is then additive.
On the other hand, for p=7,13 we have 8,14 non-singular points, hence the group can't be isomorphic to k or k* and it is therefore a nonsplit multiplicative singular reduction.

Finally, for p=19 we have 18 non-singular points, hence the group is isomorphic to (F_19)* and the singular reduction is split multiplicative.

Exercise 9: Check (with the documentation of the 'local_data' method of 'E2') that the following gives a result that is consistent with your previous answer.

```
[(p,E2.local_data(p).bad_reduction_type()) for p in prime_range(50)]
```

```
[(2, None),
 (3, 0),
 (5, None),
 (7, -1),
 (11, None),
 (13, -1),
 (17, None),
 (19, 1),
 (23, None),
 (29, None),
 (31, None),
 (37, None),
 (41, None),
 (43, None),
 (47, None)]
```

Answer: (just explain with text, so no sage-commands)

From the documentation found at https://doc.sagemath.org/html/en/reference/curves/sage/schemes/elliptic_curves/ell_local_data.html, we see that 1 corresponds to a bad split multiplicative reduction, -1 to a bad non-split multiplicative reduction and 0 to a bad additive reduction.

The Frobenius endomorphism

In the following exercises, use the following results, which were proven in the lecture at least when q is prime.

Let E be an elliptic curve and $f \in \mathrm{End}(E)$.

1. Then there exist a unique $\widehat{f} \in \mathrm{End}(E)$ (the *dual endomorphism*) given by $f\widehat{f} = \widehat{f}f = [\deg(f)]$.
2. There exists a unique $t = t(f) \in \mathbf{Z}$ (the *trace* of f) such that $f + \widehat{f} = [t]$.
3. We have $f^2 - [t]f + [\deg(f)] = [0]$.

Let $q = p^n$ be a prime power, and let E be an elliptic curve over $\mathbf{F}_q$.

A. There is an endomorphism $\mathrm{Frob}_q \in \mathrm{End}(E)$ (*the q-th power Frobenius endomorphism*) given by $\mathrm{Frob}_q(x, y) = (x^q, y^q)$.
B. We have $\deg(\mathrm{Frob}_q) = q$.
C. We have $\#E(\mathbf{F}_q) = \deg(\mathrm{Frob}_q - [1]) = q + 1 - t(\mathrm{Frob}_q)$.

We compute the number of points on E_2 over the field of 5^n elements for n from 1 to 20.

```
[E2.base_extend(GF(5^n,'x')).cardinality() for n in range(1,21)]
```

```
[8,
 32,
 104,
 640,
 3208,
 15392,
 78184,
 391680,
 1950728,
 9765152,
 48841064,
 244117120,
 1220685448,
 6103668512,
 30517360744,
 152587560960,
 762941199368,
 3814695421472,
 19073481285224,
 95367450947200]
```

Let $\overline{E_2}$ denote the reduction of E_2 modulo 5. The result of Exercise 6 shows that $\overline{E_2}$ is an elliptic curve over the field $\mathbf{F}_5$ of 5 elements

Exercise 10: Use the number of points of $\overline{E_2}$ over $\mathbf{F}_5$ to show that in $\mathrm{End}(\overline{E_2})$, we have $\mathrm{Frob}_5 = [-1] + \phi$ for some endomorphism ϕ with $\phi^2 = [-4]$. [Hint: first compute a quadratic polynomial of which Frob_5 is a root; then take $\phi = \mathrm{Frob}_5 + [1]$.]

Answer: (just text, no Sage)

First, we note $\deg(Frob_5) = 5$ and from the above list we have $\#E(F_5) = 8$. Substituting this into the equation in point C above gives $t(Frob_5) = -2$. Following the hint we set $\phi := Frob_5 + [1]$. The equation of $Frob_5$ is given by the polynomial $x^2 + 2x + 5 = 0$, hence $\phi^2 = (Frob_5 + [1])^2 = [-4]$.

Exercise 11: Use the result of Exercise 10 to give a formula for the number of points on E_2 over the field of 5^n elements. Check that your answer agrees with the list computed above for n from 1 to 20. [Hint: give an embedding $\mathbf{Z}[\phi] \to \mathbf{C}$ and show that taking dual endomorphisms corresponds to complex conjugation. Then what is the trace?]

Answer:

We have that $\phi^2 = [-4]$, thus $\deg(\phi^2) = 16$ and $\deg(\phi) = 4$. Since $\phi \circ (-\phi) = [4]$, this implies $\hat{\phi} = -\phi$. From this and the description of the embedding we are about to give it will be obvious that taking duals corresponds to taking conjugates.

Let's consider the embedding $\mathbb{Z}[\phi] \to \mathbb{C}$ given by $[1] \mapsto 1$ and $\phi \mapsto 2i$. It exists because $\phi^2 = [-4] \mapsto -4$. Now, for any $g \in \mathbb{Z}[\phi]$ the trace is given by the image of $g + \hat{g}$. This is because, if $g = \sum_j [a_j]\phi^j$, then $\hat{g} = \sum_j [(-1)^j a_j]\phi^j$ and $g + \hat{g} = \sum_j [a_{2j}]\phi^{2j} = \sum_j [(-4)^j a_{2j}] \mapsto \sum_j (-4)^j a_{2j}$, which is precisely the trace.

From the previous exercise, $\#E(\mathbb{F}_q) = q + 1 - t(Frob_q)$. Set $f := Frob_5$. We have $f^n = Frob_5^n = Frob_{5^n}$ and through the embedding we will compute $t(f^n) = t((\phi + [-1])^n)$.

Since $f^n + \hat{f^n} = (\phi + [-1])^n + (-\phi + [-1])^n \mapsto (-1 + 2i)^n + (-1 - 2i)^n$. We know that $-1 + 2i = \sqrt{5}(\cos(\theta) + i \cdot \sin(\theta))$ with $\theta = \arg(-1 + 2i)$. It follows that $f^n + \hat{f^n} \mapsto 2 \cdot 5^{n/2} \cos(n\theta)$.

It follows that $t = 2 \cdot 5^{n/2} \cos(n\theta)$, but it is also equal to $2 \sum_k \binom{n}{2k} (-1)^{n-2k} (2i)^k$.

```
r = 0
for n in range(1,21):
    for j in range(floor(n/2)+1):
        r+=binomial(n,2*j)*(-4)^j*(-1)^n
    print(5^n-2*r+1)
```

```
8
34
112
626
3208
15474
78032
391586
1951688
9763714
48839152
244128146
1220672968
6103638354
30517483472
152587466306
762940775048
3814696743394
19073480762992
95367445382066
```

We see that these values coincide with the cardinality of $E_2(\mathbb{F}_{5^n})$.

Exercise 12: For $p = 23$, is there for every N in the Hasse-Weil interval

$$[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$$

an elliptic curve C over $\mathbb{F}_p$ with $\#C(\mathbb{F}_p) = N$?

Answer:

The interval is described as:

```
(23-2*sqrt(23)+1).n(), (23+2*sqrt(23)+1).n()
```

```
(14.4083369533746, 33.5916630466254)
```

The possible values of $\#C(\mathbb{F}_{23})$ are given by the integers from 15 to 33.

```
F = GF(23)
ord = []
for a in F:
    for b in F:
        if 4*a^3+27*b^2!=0:
            E = EllipticCurve(F, [a,b])
            if E.order() not in ord:
                ord+=[E.order()]
sorted(ord)
```

```
[15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31,
32, 33]
```

By studying all of the possible elliptic curves over $\mathbb{F}_{23}$ and computing their orders we get this list, which contains every integer from 15 to 33.

Back to top

Mordell-Weil groups

Exercise 13: Compute the rank of the curve $y^2 = x^3 + a$ for $a \in \{1, \ldots, 50\}$.

Answer:

```
[(a,EllipticCurve([0,a]).rank()) for a in range(1,51)]
```

```
[(1, 0),
 (2, 1),
 (3, 1),
 (4, 0),
 (5, 1),
 (6, 0),
 (7, 0),
 (8, 1),
 (9, 1),
 (10, 1),
 (11, 1),
 (12, 1),
 (13, 0),
 (14, 0),
 (15, 2),
 (16, 0),
 (17, 2),
 (18, 1),
 (19, 1),
 (20, 0),
 (21, 0),
 (22, 1),
 (23, 0),
 (24, 2),
 (25, 0),
 (26, 1),
 (27, 0),
 (28, 1),
 (29, 0),
 (30, 1),
 (31, 1),
 (32, 0),
 (33, 1),
 (34, 0),
 (35, 1),
 (36, 1),
 (37, 2),
 (38, 1),
 (39, 1),
 (40, 1),
 (41, 1),
 (42, 0),
 (43, 2),
 (44, 1),
 (45, 0),
 (46, 1),
 (47, 1),
 (48, 1),
 (49, 0),
 (50, 1)]
```

Exercise 14: What is the smallest integer $a > 0$ for which the rank of the Mordell-Weil group of the curve $y^2 = x^3 + a$ is at least 3?

Answer:

```
a = 1
while (EllipticCurve([0,a]).rank() < 3):
    a+=1
print "The minimum value of a is:", a
```

```
The minimum value of a is: 113
```

Back to top

Period lattices

Exercise 15: For the elliptic curve $E : y^2 = x^3 + 5$ find numerical approximations of a basis of a lattice L in the complex numbers $\mathbb{C}$, such that $\mathbb{C}/L$ is isomorphic to E. Hint: use E.period_lattice.

Answer:

```
E = EllipticCurve(QQ,[0,5])
L = E.period_lattice()
b = L.basis()
print "A basis is given by:", b
```

```
A basis is given by: (3.21684899174839, 1.60842449587419 +
0.928624315664154*I)
```

The elliptic curve given by $y^2 = x^3 + 5$ has an automorphism $\rho : (x, y) \mapsto (\zeta_3 x, y)$, where $\zeta_3 = \exp(2\pi i/3)$ is a primitive 3rd root of unity. Since ρ is not $[\pm 1]$, this implies that the endomorphism ring is strictly larger than $\mathbf{Z}$. If the endomorphism ring of an elliptic curve is larger than $\mathbf{Z}$, then we say that the elliptic curve has *complex multiplication*. By the equivalence of categories from the lecture on complex elliptic curves, this implies that the lattice has a multiplier ring that is larger than $\mathbf{Z}$ and in particular (see the exercises from that lecture) is an imaginary quadratic order. The lattice is a scaled version of an ideal of that order.

Exercise 16: Use the function `algdep` to find an exact formula for a basis of a scaled version of the lattice L.

Answer:

```
p = algdep(b[1]/b[0],2)
p
```

```
3*x^2 - 3*x + 1
```

The polynomial $3x^2 - 3x + 1$ has roots $\frac{3+\sqrt{-3}}{6}$, hence the scaled lattice L is given by $\mathbb{Z} + \frac{3+\sqrt{-3}}{6}\mathbb{Z}$ and it has a basis given by $(1, \frac{3+\sqrt{-3}}{6})$.

Back to top

Porism of Diophantus

Diophantus proved that if a postive rational number d is the difference of two rational positive cubes, then it is also the sum of two rational positive cubes. For instance, since $7 = 2^3 - 1^3$, there should also be positive rational numbers x and y with $x^3 + y^3 = 7$. Indeed, one has $(\frac{4}{3})^3 + (\frac{5}{3})^3 = 7$.

We consider the projective curve given by $x^3 + y^3 = dz^3$ with the point $[1 : -1 : 0]$ and make a substitution to obtain a Weierstrass model of the elliptic curve.

```
P2.<x,y,z> = ProjectiveSpace(QQ,2)
d=7
cubic = x^3 + y^3 - d*z^3
```

```
P = [1,-1,0]
phi = EllipticCurve_from_cubic(cubic, P); phi
```

```
Scheme morphism:
  From: Closed subscheme of Projective Space of dimension 2 over
Rational Field defined by:
  x^3 + y^3 - 7*z^3
  To:   Elliptic Curve defined by y^2 + 2*x*y - 7/3*y = x^3 - x^2 +
7/3*x - 49/27 over Rational Field
  Defn: Defined on coordinates by sending (x : y : z) to
        (-z : -y + z : -3/7*x - 3/7*y)
```

```
C = Curve(phi.domain())
E = phi.codomain()
psi = phi.inverse()
```

```
# The elliptic curve above is not given by a nice short Weierstrass equation with integer coefficients.
# By modifying the morphism above, you could get such a nicer equation.
# Uncomment the following lines if one of the commands above gave an error.
#C=Curve(cubic)
#E=EllipticCurve([0,-432*d^2])
#transformation=[(36*d*z-y)/(72*d),(36*d*z+y)/(72*d),x/(12*d)]
#D=Curve(E)
#psi = hom(D,C,transformation)
#psi
```

Feel free to plot the curves, but please delete the plots before printing or making a pdf (to save paper).

We can check that the transformation does indeed map E to C by doing a substitution.

```
f=C.defining_polynomial()
g=E.defining_polynomial()
f(list(psi)) / g;
```

```
Traceback (click to the left of this block for traceback)
...
TypeError: 'list' object is not callable
```

Exercise 17:

a) How can we obtain the solution $\{x, y\} = \{\frac{4}{3}, \frac{5}{3}\}$ from the solution $\{x, y\} = \{2, -1\}$?

b) Find positive rational x, y, other than $\{x, y\} = \{\frac{4}{3}, \frac{5}{3}\}$ with $x^3 + y^3 = 7$.

Answer:

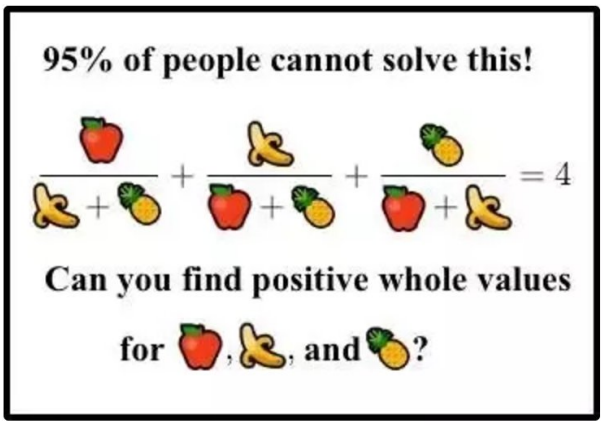
(a) Consider $Q = \phi([2 : -1 : 1]) \in E$, then $2Q \in E$. We have then that $\psi(2Q) = [5/3 : 4/3 : 1] \in C$ and, since the equation of C is symmetric in X and Y, we have that $[4/3 : 5/3 : 1] \in C$.

(b) From (a) we have that $(5/3)^2 + (4/3)^2 = (4/3)^2 + (5/3)^2 = 7$ hence $[5/3 : 4/3 : 1]$ provides the new solution we are looking for.

Another Diophantine equation

Exercise 18:

Solve the following internet meme problem.



Answer:

Denoting the apple by x, the banana by y and the pineapple by z, getting rid of the denominators, we get the equation $x^3+y^3+z^3-3x^2y-3x^2z-3xy^2-3y^2z-3xz^2-3yz^2-5xyz=0$

```
gP2.<x,y,z> = ProjectiveSpace(QQ,2)
cubic = x^3+y^3+z^3-3*x^2*y-3*x^2*z-3*x*y^2-3*y^2*z-3*x*z^2-3*y*z^2-5*x*y*z

P = [1,-1,0]
phi = EllipticCurve_from_cubic(cubic, P)
phi
```

```
Scheme morphism:
  From: Closed subscheme of Projective Space of dimension 2 over
Rational Field defined by:
  x^3 - 3*x^2*y - 3*x*y^2 + y^3 - 3*x^2*z - 5*x*y*z - 3*y^2*z -
3*x*z^2 - 3*y*z^2 + z^3
  To:   Elliptic Curve defined by y^2 + x*y + 91/6*y = x^3 +
47/2*x^2 - 637/12*x - 8281/216 over Rational Field
  Defn: Defined on coordinates by sending (x : y : z) to
        (-1/6*z : -y + 1/6*z : 6/91*x + 6/91*y - 1/91*z)
```

```
C = Curve(phi.domain())
E = phi.codomain()
psi = phi.inverse()
```

By trial and error, we find the point $P=[-4:-11:1]$ on the cubic. By looking at $\phi(P)$ we get a point on the elliptic curve E. By looking at $\psi(n\cdot\phi(P))$ we then find other solutions of the considered equation. With the following code we will bruteforce this process.

```
Q=phi([-4,-11,1])
m = 0
n = 0
while n==0:
    if psi(m*Q)[0]>0 and psi(m*Q)[1]>0:
        R = psi(m*Q)
        x = R[0]
        y = R[1]
        z = R[2]
        print (R[0].numerator()*R[1].denominator(),R[1].numerator()*R[0].numerator(),R[0].denominator()*R[1].denominator())
        n = 1
    else: m+=1
```

```
(16127754391509855521072098080973888216673380401866645733821054782267623274501894697047525583569505407029777200060848575320401503169350149754298183345012598884
4,
569635243689575396521942232673167962846376168837264424950327093868558287554993176009246759841537575754842098681453772800876441710858447366606862171694608190642
1,
497542981833450125988844,
569635243689575396521942232673167962846376168837264424950327093868558287554993176009246759841537575754842098681453772800876441710858447366606862171694608190642
1,
828755499317600924675984153757575484209868145377280087644171085844,
666068621716946081906421,
191284878565386305300167031744205143774973513447310666584402378510377002969945401446257337502058412389549828486391632513958677641484087876881091691336635852964,
700296994540144625733750205841238954982848639163251395867764148408,
768810916913663585296)
```

We see that this one provides us a positive integer solution of our original problem, that is
$x=16127754391509855521072098080973888216673380401866645733821054782267623274501894697047525583569505407029777200060848575320401503169350149754298183345012598884

368751317941299998271978115652254748254929799689719709962831374716372246340555 79,
y=569635243689575396521942232673167962846376168837264424950327093868558287554993176009246759841537575754842098681453772800876441710858447366606862171694608190642
1,
z=191284878565386305300167031744205143774973513447310666584402378510377002969945401446257337502058412389549828486391632513958677641484087876881091691336635852964$

Let's check that it is indeed a solution:

```
x/(y+z)+y/(x+z)+z/(x+y)==4
```

```
True
```

Back to top

Modularity

Exercise 19 For any prime p, let N_p denote the number of points on the Weierstrass curve given by $y^2=x^3-4x^2+16$ over $\mathbb{F}_p$. Let M_n denote the coefficient of q^n in the formal power series expansion of the infinite product

$$q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2.$$

Compute M_p+N_p for all primes p up to 100. Conjecture what M_p+N_p equals for primes $p>100$.

Here are some examples of how to work with power series:

Answer:

```
E3 = EllipticCurve(QQ,[0,-4,0,0,16])
R.<q> = QQ[[]]
f = q
for n in range(1,101):
    f = f * (1-q^n)^2 * (1-q^(11*n))^2
[(p, E3.Np(p) + f.list()[p]) for p in prime_range(100)]
```

```
[(2, 3),
 (3, 4),
 (5, 6),
 (7, 8),
 (11, 12),
 (13, 14),
 (17, 18),
 (19, 20),
 (23, 24),
 (29, 30),
 (31, 32),
 (37, 38),
 (41, 42),
 (43, 44),
 (47, 48),
 (53, 54),
 (59, 60),
 (61, 62),
 (67, 68),
 (71, 72),
 (73, 74),
 (79, 80),
 (83, 84),
 (89, 90),
 (97, 98)]
```

We conjecture that $M_p+N_p=p+1$ for every prime $p>100$.

Back to top

Heights

Given a Weierstrass model of an elliptic curve C over $\mathbb{Q}$, we define the *naive logarithmic height* of a rational point $P\in C(\mathbb{Q})$ by

$$h_{\mathrm{n}}(P) = \log(\max(|d|, |n|)),$$

with $d, n \in \mathbb{Z}$ such that $\gcd(d, n) = 1$ and $x(P) = \frac{d}{n}$.

Exercise 20: Take your favourite elliptic curve in short Weierstrass form with a point P of infinite order. For $m \in \{1, \ldots, 100\}$, compute the square root of $h_{\mathrm{n}}(mP)$. How do the values seem to grow asymptotically?

Answer:

First we shall define an amazing elliptic curve:

```
FE = EllipticCurve(QQ, [0,57])
print FE
P = FE([4,11])
P
print "Order of P:", P.order()
```

```
Elliptic Curve defined by y^2 = x^3 + 57 over Rational Field
Order of P: +Infinity
```

We see that the point P belongs to my favourite elliptic curve and it has infinite order. We will then compute the height of $n \cdot P$ for n ranging from 1 to 100, as required.

```
list = []
for n in range(1,101):
    j=sqrt(log(max(abs((n*P)[0].numerator()), abs((n*P)[0].denominator())))).n()
    list+=[(n,j)]
list
```

```
[(1, 1.17741002251547),
 (2, 2.44361654925450),
 (3, 3.48775541297736),
 (4, 5.01664710828326),
 (5, 6.25675225578753),
 (6, 7.35439301421151),
 (7, 8.70951780045525),
 (8, 9.95930564813766),
 (9, 11.2146322741888),
 (10, 12.4547339050373),
 (11, 13.6975254157891),
 (12, 14.8922038159149),
 (13, 16.2087162184005),
 (14, 17.4546006794269),
 (15, 18.6425777923660),
 (16, 19.9317719931161),
 (17, 21.1784040595783),
 (18, 22.4292645483774),
 (19, 23.6725599913022),
 (20, 24.9160290598823),
 (21, 26.1328718425659),
 (22, 27.4192295061282),
 (23, 28.6655744413109),
 (24, 29.8754123673799),
 (25, 31.1485277468962),
 (26, 32.3944032115657),
 (27, 33.6438968225649),
 (28, 34.8883277546743),
 (29, 36.1321207083831),
 (30, 37.3578935523246),
 (31, 38.6321335428708),
 (32, 39.8786054141889),
 (33, 41.0983061041023),
 (34, 42.3641529210312),
 (35, 43.6096941825957),
 (36, 44.8585290967488),
 (37, 46.1035396244606),
 (38, 47.3475142900135),
 (39, 48.5781164557188),
 (40, 49.8458149246219),
 (41, 51.0923391659095),
 (42, 52.3176567150118),
 (43, 53.5793576276246),
 (44, 54.8247113400540),
 (45, 56.0731613709244),
 (46, 57.3185220586042),
 (47, 58.5626106709863),
 (48, 59.7962420057078),
 (49, 61.0598453553056),
 (50, 62.3063962553041),
 (51, 63.5353411777979),
 (52, 64.7943602965216),
 (53, 66.0395939661676),
 (54, 67.2877936450840),
 (55, 68.5333878125105),
 (56, 69.7775529752363),
 (57, 71.0132642091234),
 (58, 72.2740623440297),
 (59, 73.5206287351270),
 (60, 74.7521095608790),
 (61, 76.0092504325051),
 (62, 77.2544004509310),
 (63, 78.5024259192161),
 (64, 79.7481862084528),
 (65, 80.9924050388124),
 (66, 82.2296346178265),
 (67, 83.4883907003507),
 (68, 84.7349669759026),
 (69, 85.9683204192258),
 (70, 87.2240715018987),
 (71, 88.4691595638337),
 (72, 89.7170581933047),
 (73, 90.9629422401067),
 (74, 92.2071996278253),
 (75, 93.4455879608537),
 (76, 94.7027908474347),
 (77, 95.9493738997064),
 (78, 97.1841667668424),
 (79, 98.4388471585795),
 (80, 99.6838871149809),
 (81, 100.931690467329),
 (82, 102.177669924263),
 (83, 103.421955283330),
 (84, 104.661258341577),
 (85, 105.917239968910),
 (86, 107.163827948485),
 (87, 108.399761729766),
 (88, 109.653591375937),
 (89, 110.898592506619),
 (90, 112.146322741260),
 (91, 113.392377729297),
 (92, 114.636683278314),
 (93, 115.876727941196),
 (94, 117.131723985591),
 (95, 118.378315732926),
 (96, 119.615176003269),
 (97, 120.868312938129),
```

```
    (98, 122.113281674355),
    (99, 123.360955015066),
    (100, 124.607071072186)]
```

Back to top

By plotting the list of points we see that the values grow linearly.