Elliptic Curve Demo

Part I: Elliptic curves over Q

Graphs of some elliptic curves

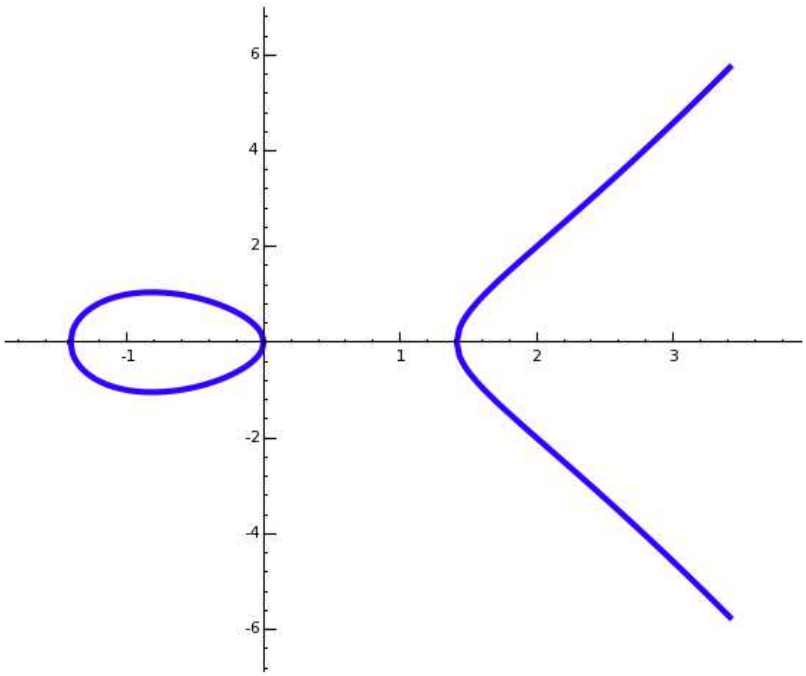
```
E = EllipticCurve([-2,0]); E
```

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

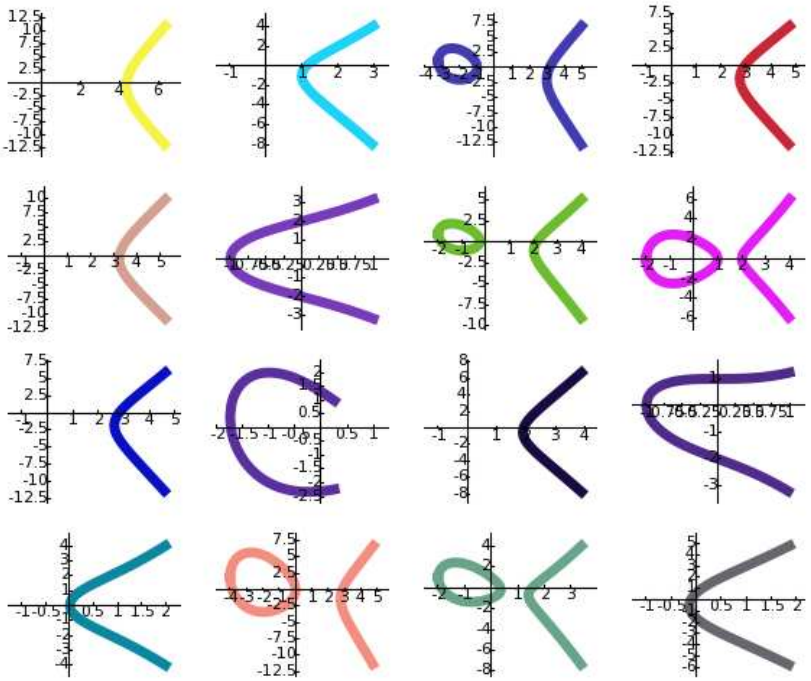
```
show(E)
```

$$y^2 = x^3 - 2x$$

```
show(plot(E, thickness=3, hue=0.7))
```




```
v = []
for E in cremona_optimal_curves(range(40)):
    v.append(plot(E, thickness=5, rgbcolor=(random(),random(),random())))
n = len(v)
m = floor(sqrt(n))
show(graphics_array(v, m, m))
```

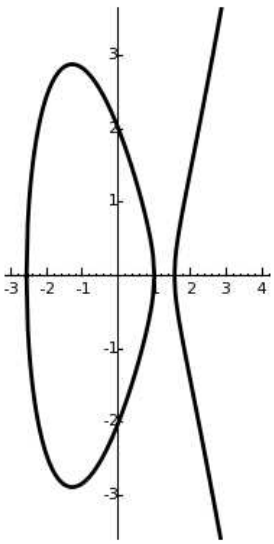


Elliptic curve group law examples

```
E = EllipticCurve([-5, 4]); E
```

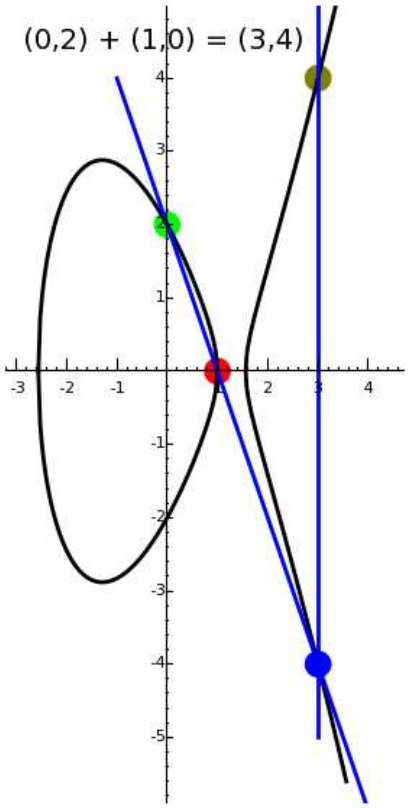
```
Elliptic Curve defined by y^2  = x^3 - 5*x + 4 over Rational Field
```

```
G = plot(E, thickness=2)
G.show(ymin=-3,ymax=3,figsize=[2,4])
```



```
P = E(1,0); Q = E(0,2); R = P+Q
print R
```

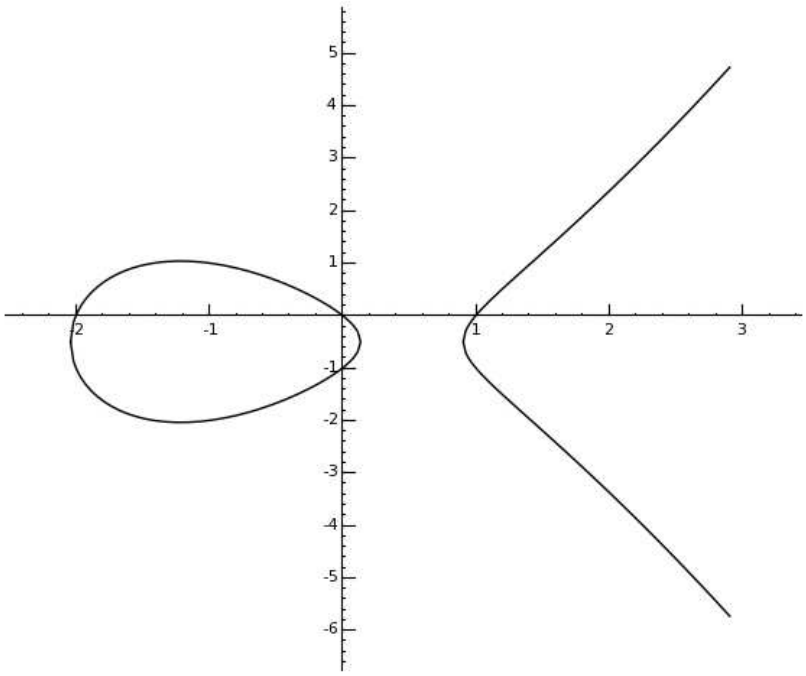
```
        (3 : 4 : 1)
def pnt(z,clr):
    return plot(z, pointsize=200, rgbcolor=clr)
show(G + pnt(P,(1,0,0)) + pnt(Q,(0,1,0)) + \
       pnt(R,(0.5,0.5,0)) + pnt(-R,(0,0,1)) + \
     line([(-1,4), (4,-6)],rgbcolor=(0,0,1),thickness=2) + \
     line([(3,-5), (3, 5)], rgbcolor=(0,0,1),thickness=2) + \
     text("(0,2) + (1,0) = (3,4)", (2.7,4.5), \
           fontsize=14, horizontal_alignment='right'), \
    figsize=[3,6], ymin=-5,ymax=4)
```



3d Graph of Rational Points

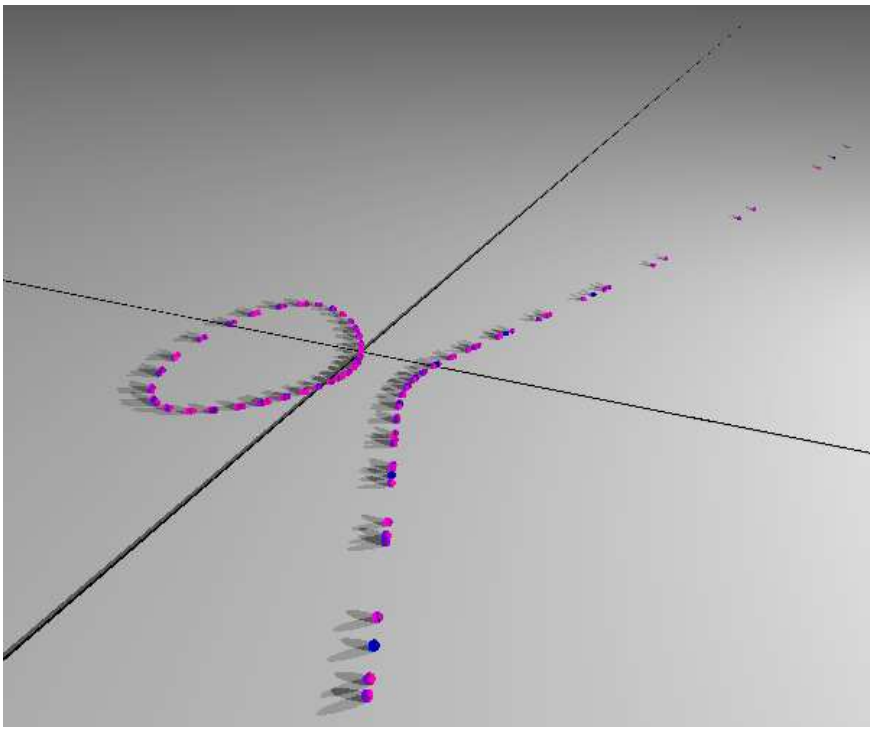
```
# This is my favorite elliptic curve
E = EllipticCurve('389a')

show(plot(E))
```




```
t = Tachyon(xres=600, yres=500, \
          camera_center=(4,7,4), look_at=(1,0,0), raydepth=4)
t.light((10,3,2), 1, (1,1,1))
t.light((10,-3,2), 1, (1,1,1))
t.texture('black', color=(0,0,0))
t.texture('red', color=(1,0,0))
t.texture('grey', ambient=1,diffuse=1, specular=0, opacity=1, color=(0.8,
t.plane((0,0,0),(0,0,1),'white')
t.cylinder((0,0,0),(1,0,0),.01,'black')
t.cylinder((0,0,0),(0,1,0),.01,'black')
E = EllipticCurve('389a')
G = E.gens()
n = 6
for i in range(-n,n+1):
  for j in range(-n,n+1):
    if i == 0 and j == 0: continue
    Q = i*G[0] + j*G[1]
    t.texture('r%s'%i,color=(float(i)/n, 0, float(j)/n))
    t.sphere((Q[0], -Q[1], .02), .04, 'r%s'%i)

t.save('sage.png')    # long time, seconds
```



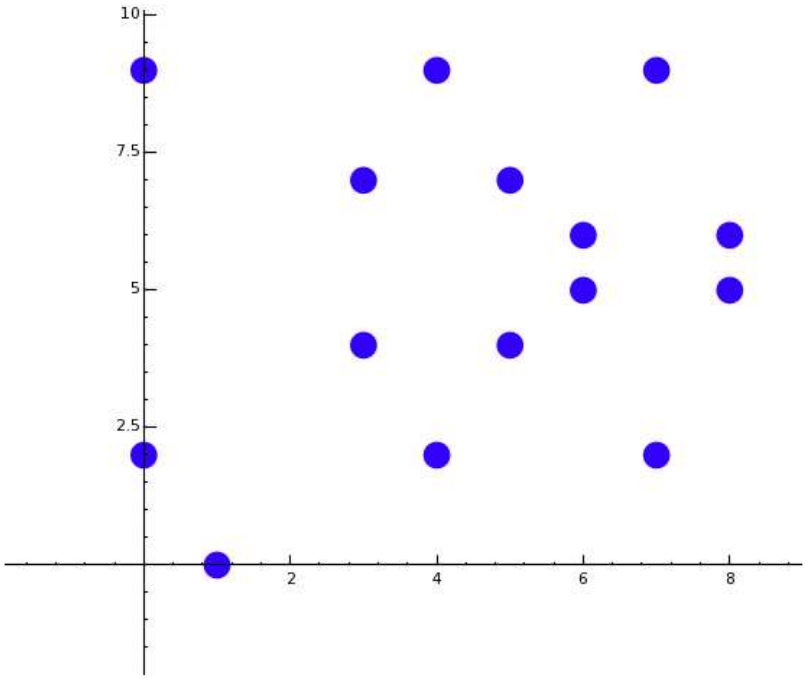
```
# The rational points get quite large.
P = E(0,0)
show([n*P for n in range(15)])
```

$$\left[(0 : 1 : 0),\ (0 : 0 : 1),\ (3 : 5 : 1),\ \left(-\frac{11}{9} : \frac{28}{27} : 1\right),\ \left(\frac{114}{121} : -\frac{267}{1331} : 1\right),\ \left(-\frac{2739}{1444} : -\frac{77033}{54872} : 1\right),\ \left(\frac{89566}{62001} : -\frac{31944320}{15438249} : 1\right),\ \left(-\frac{2182983}{5555449} : -\frac{20464084173}{13094193293} : 1\right),\ \left(\frac{1169154495}{76860289} : -\frac{41440508823358}{673834153663} : 1\right),\ \left(-\frac{33046084324}{246050721225} : -\frac{55777095075809107}{122049769502842875} : 1\right),\ \left(\frac{148390875719505}{14208165274384} : \frac{184971133466146499305 5}{53555860356635366848} : 1\right),\ \left(-\frac{45474259258888548}{89493141443245849} : \frac{182148930686659226620802 00}{26772235083517850771317507} : 1\right),\ \left(\frac{189342513653835405031}{145543651499666674881} : \frac{130265686289061928855175 6451671}{17558600588589201051459277892 79} : 1\right),\ \left(-\frac{791464517307769165158639}{400595921638177470929689} : \frac{321257461162480677512541268853292 24}{253547764228101693293432324785359613} : 1\right),\ \left(\frac{421716559923819829142368 3014}{430397393292454710068640624 1} : -\frac{264617954559570241918160421125405948501249}{282360829154337216405120742020728661106961} : 1\right)\right],$$

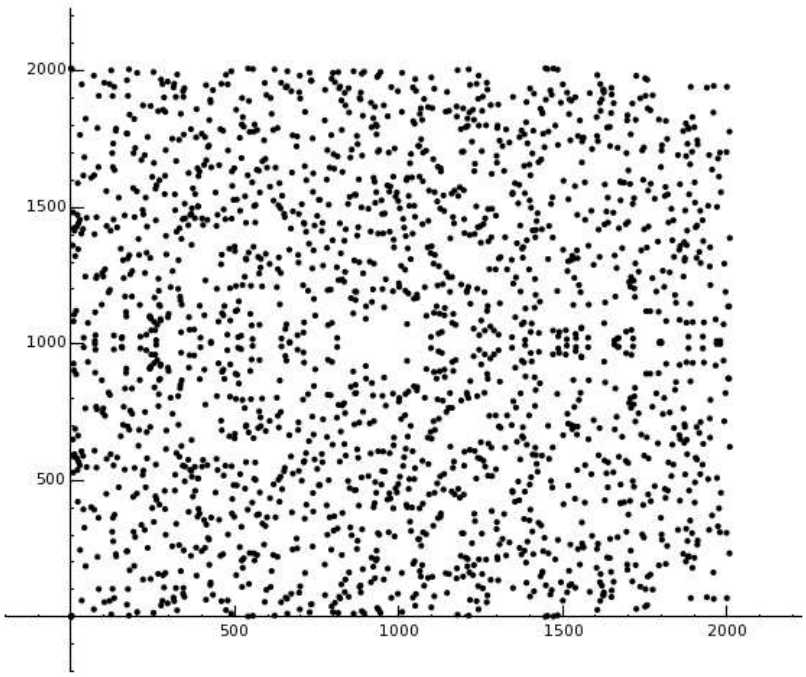
Part II: Elliptic curves modulo p

Graph of Set of Points modulo p

```
E = EllipticCurve(GF(11), [-5,4]); E
```
```
        Elliptic Curve defined by y^2  = x^3 + 6*x + 4 over Finite Field o
```
```
show(plot(E,pointsize=200,hue=.7))
```




```
E = EllipticCurve(GF(2011), [-5,4]); E
```
```
        Elliptic Curve defined by y^2  = x^3 + 2006*x + 4 over Finite Fiel
```
```
show(plot(E))
```



Arithmetic on elliptic curve modulo p

```
E = EllipticCurve(GF(19), [-5, 4])
P = E(1,0); Q = E(0,2)

P +  Q
        (3 : 4 : 1)
7*Q
        (16 : 7 : 1)
P + Q + Q  + Q
        (15 : 6 : 1)
```

Diffie Hellman key exchange on elliptic curve modulo p

```
p = 78596310237942882237669478944689739620749856895l
show(p.str(16))

                    89abcdef012345672718281831415926141424f7

E = EllipticCurve(GF(p), [3176890812513255034763174764138276932727469559
   790528966078787587181205720257185354321006519341])
E
        Elliptic Curve defined by y^2  = x^3 +
        3176890812513255034763174764138276932727469559271*x +
        790528966078787587181205720257185354321006519341 over Finite Field
        785963102379428822376694789446897396207498568951
time s = E.cardinality()
s
        785963102379428822376693024881714957612686157429
        CPU time: 0.00 s,  Wall time: 0.01 s
is_prime(s)
        True
B = E(771507216262649826170648268565579889907769254176, \
      390157510246556628525279459266514995562533196655)
```

```
%time
# Do Diffie-Hellman with this
n = randint(2,s)
m = randint(2,s)
Sm = m*(n*B)
Sn = n*(m*B)
```

```
CPU time: 0.10 s,  Wall time: 0.12 s
```

```
Sm
```

```
(153470721398328205142504643349771892468236940170 :
132434024879389525183838911880841584368869098553 : 1)
```

```
Sn
```

```
(153470721398328205142504643349771892468236940170 :
132434024879389525183838911880841584368869098553 : 1)
```