2014-02-03.sagews

February 10, 2014

Contents

1 February 3, 2014: Elliptic Curves

- Feb 3 whiteboard: `http://youtu.be/YRX3nAhBzCw`
- Feb 5 whiteboard: `http://youtu.be/EQPQr1kuA3E`
- Feb 7 screencast: `http://youtu.be/ODagXOOdYUY`

1.1 Whiteboard

- Linear equations (one equation)
- Quadratic equations (one equation): Pythagorean triples and that you can enumerate them (how=homework)
- Cubic equations: um, a little bit harder than linear and quadratic focus on elliptic curves for now

1.2 Elliptic Curve Examples

1.2.1 An Elliptic Curve over Q

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

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

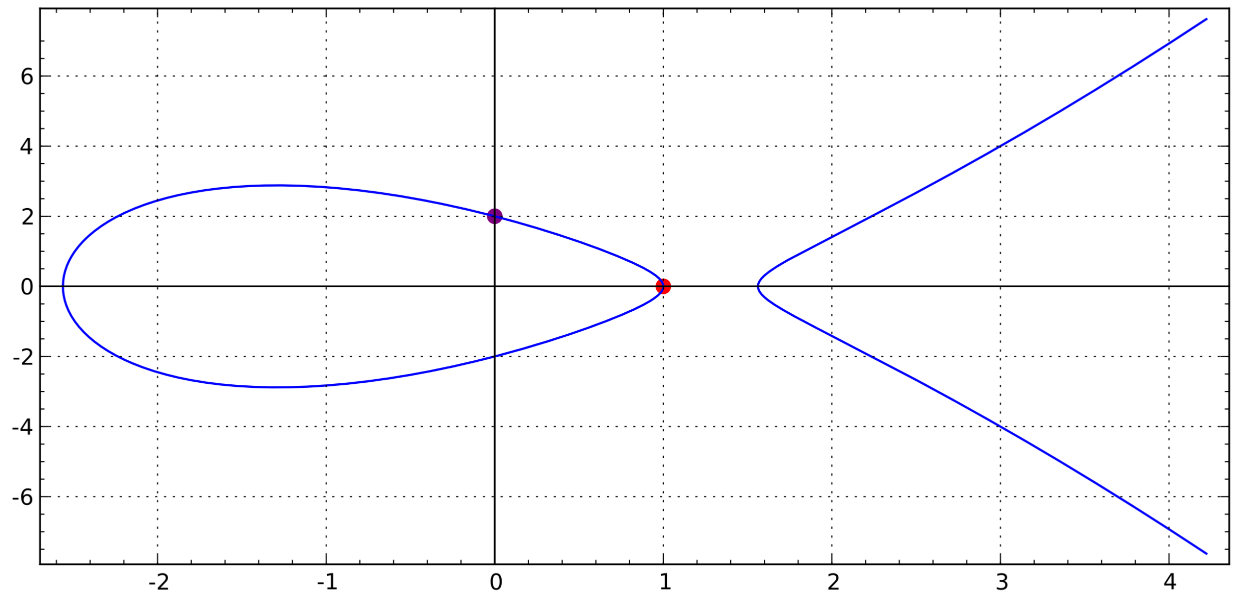
```
# zero element of the group
E(0)
```

```
(0 : 1 : 0)
```

```
# two points
P = E([1,0]); Q = E([0,2])
print "P =", P
print "Q =", Q
```

```
P = (1 : 0 : 1)
Q = (0 : 2 : 1)
```

```
g = plot(E) + point(P[:2],color='red',pointsize=50) + point(Q[:2],color='\
    purple',pointsize=50)
g.show(svg=True, frame=True, gridlines=True)
```




```
P+Q
```

```
(3 : 4 : 1)
```

```
4*Q
```

```
(352225/576 : 209039023/13824 : 1)
```

```
# y^2 = x^3 - 5*x + 4
(209039023/13824)^2 == (352225/576)^3 - 5*(352225/576) + 4
```

```
True
```

```
8*Q
```

```
16*Q
```

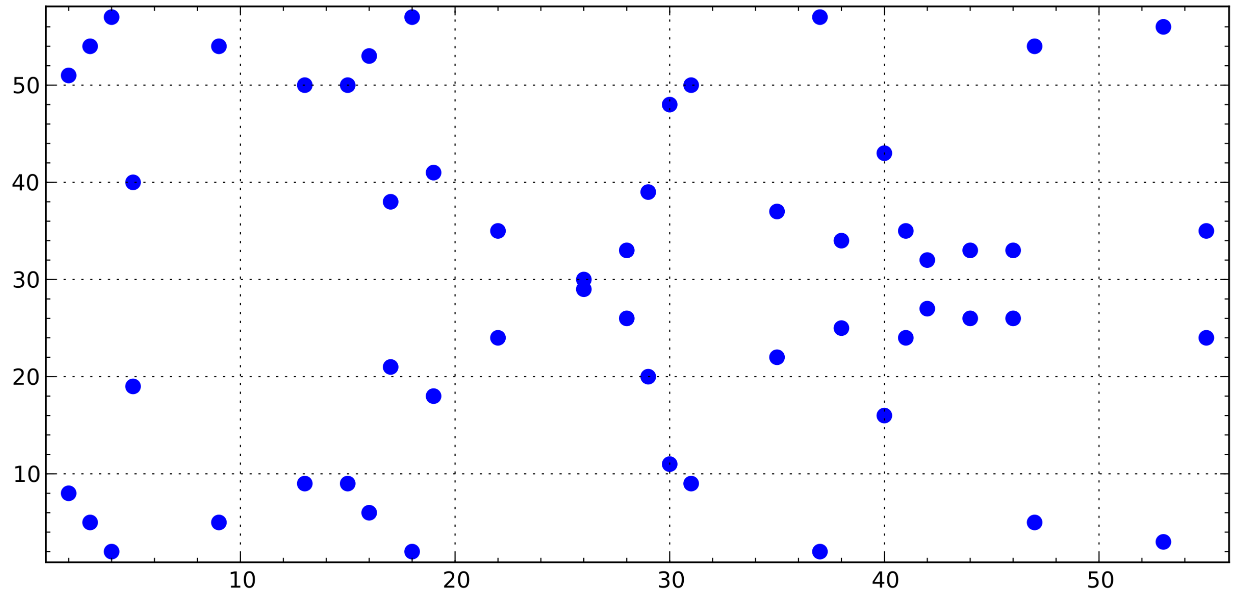
```
32*Q
```

1.2.2 An Elliptic Curve Modulo p

```
E = EllipticCurve(Integers(59), [1,54])
E
```

```
Elliptic Curve defined by y^2 = x^3 + x + 54 over Ring of integers modulo 59
```

```
E.plot(pointsize=50).show(gridlines=True, svg=True, frame=True)
```



```
E.cardinality()
```

```
57
```

```
P = E.points()[5]; Q = E.points()[7]
print "P =", P
print "Q =", Q
```

```
P = (4 : 2 : 1)
Q = (5 : 19 : 1)
```

```
P + Q
```

```
(44 : 26 : 1)
```

1.2.3 Things to come:

- Elliptic curves modulo a huge prime p for creating cryptosystems
- Fake elliptic curves modulo a composite number $n = pm$ for trying to factor
- Elliptic curves over the rational numbers for understanding Diophantine equations such as the one in Fermats Last Theorem