2014-02-10.sagews

February 10, 2014

Contents

1 February 10, 2014: Elliptic Curves Cryptography

1.1 Computational verification that the group law is associative (over Q, for distinct points).

Our curve is $y^2 = x^3 + ax + b$ and the three points are $(x_1, y_1), (x_2, y_2), (x_3, y_3)$.

```
# Create the polynomial ring in x1-y3 and a,b
R.<x1,y1,x2,y2,x3,y3,a,b> = QQ[]
R
```

```
Multivariate Polynomial Ring in x1, y1, x2, y2, x3, y3, a, b over Rational Field
```

```
# Impose relations
rels = [y1^2 - (x1^3 + a*x1 + b), y2^2 - (x2^3 + a*x2 + b), y3^2 - (x3^3 \
   + a*x3 + b)]
Q = R.quotient(rels)
Q
```

```
Quotient of Multivariate Polynomial Ring in x1, y1, x2, y2, x3, y3, a, b over Rational
Field by the ideal (-x1^3 + y1^2 - x1*a - b, -x2^3 + y2^2 - x2*a - b, -x3^3 + y3^2 - x3*a
- b)
```

```
# Define group operation (assumes points *distinct*)
def op(P1,P2):
    x1,y1 = P1
    x2,y2 = P2
    lam = (y1-y2)/(x1-x2)
    nu  = y1-lam*x1
    x3  = lam^2 - x1 - x2
    y3  = -lam*x3 - nu
    return (x3, y3)
```

```
# Define points and add them associating both ways
P1 = (x1,y1); P2 = (x2,y2); P3 = (x3,y3)
```

```
Z = op(P1, op(P2,P3)); W = op(op(P1,P2),P3)
```

```
# Check that Z and W define the same point
(Q(Z[0].numerator()*W[0].denominator() - Z[0].denominator()*W[0].\
   numerator())) == 0
(Q(Z[1].numerator()*W[1].denominator() - Z[1].denominator()*W[1].\
   numerator())) == 0
```

```
True
True
```

1.2 Next, well talk about 2014-02-07.sagews (Diffie-Hellman)