University College London
Department of Computer Science

Cryptanalysis Lab 05

J. P. Bootle, N. Courtois

March 6, 2019

jonathan.bootle.14@ucl.ac.uk
Version 2.0

1. Elliptic Curves

Click on the green letter in front of each sub-question (e.g. (a)) to see a solution. Click on the green square at the end of the solution to go back to the questions.

Exercise 1. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Write $+$ for the operation of adding two points. Beware: $P + Q \neq (x_1 + x_2, y_1 + y_2)$!

(a) Watch the tutorial on elliptic curve point addition at https://www.youtube.com/watch?v=XmygBPb7DPM.

(b) Browse the internet to find the formulae for the coordinates of $P + Q$ when $P \neq Q$. What about when $P = Q$? You can assume that $Q \neq (x_1, -y_1)$ since things are slightly different in this case.

(c) Let $E : y^2 = x^3 + 3x + 3$ be an elliptic curve, defined over $\mathbb{F}_7$. Two points on the curve are $P = (4, 3)$ and $Q = (3, 2)$. Verify that $2^*P = Q$ (remember that $2^*P = P + P$).

(d) Construct E, P, Q in SAGE using the following commands. Check your answer to the previous part by typing $2 * P$ (the answer will have three coordinates, we ignore the last coordinate). What is

$P + Q$?

```
p = 7
E = EllipticCurve( GF(p),[3,3] )
P = E(4,3)
Q = E(3,2)
```

(e) Type $E.cardinality()$ to find out how many points lie on this elliptic curve.

(f) Type $E.gens()$ to obtain a set of points which generate all points in the elliptic curve group.

2. Bitcoin Elliptic Curve

We recall that

Theorem: [Hasse 1930s] For any elliptic curve

$$|\#E(F_p)) - p + 1| \leq 2\sqrt{p}$$

In bitcoin elliptic curve we have
p=115792089237316195423570985008687907853269984665640564039457584007908834671663
and

q=115792089237316195423570985008687907852837564279074904382605163141518161494337.

Compute in SAGE:

$$\frac{p-q}{\sqrt{p}}$$

3. Graphs For Elliptic Curves

```
p=109; E = EllipticCurve(FiniteField(p), [103,3]); P = plot(E

p=103; E = EllipticCurve(FiniteField(p), [41,19]); P = plot(E

p=next_prime(120);p
E = EllipticCurve(FiniteField(p), [13,14]);
P = plot(E, rgbcolor=(1,0,1)); P
E.cardinality()
```

4. Sub-Groups in Elliptic Curves

Let $p = 71$. Consider the curve $E = E(\mathbb{F}_p)$ defined by

$$y^2 = x^3 + x + 28$$

Q1: Determine the number of points on E.

Q2: Show that E is not a cyclic group.

Q3: Could this curve be used or adapted to be used in crypto (as a very small size example)? Based on Lagrange theorem propose a method to insure we get a cyclic group for cryptographic applications.

Q4: What is the order of E(4,5)?

Q5: What is the maximum order of an element in E? Find an element having this order.

Q6: What is the minimum order of an element in E excluding the neutral point? Find an element having this order.

Q7: Which points are 2-torsion points? Which points are torsion points?

Some code fragments which can help:

```
E = EllipticCurve(GF(?), [?,28]); E.cardinality()
[ E.random_point().order() for n in range(1,10) ]
```

5. Sub-Groups and Rational Mappings and Polynomials - Important for Project D73

Consider an elliptic curve $E(\mathbb{F}_p)$ defined by

$$y^2 = x^3 + ax + b$$

where $4a^3 + 27b^2 \neq 0 \mod p$ and $p > 3$ is a prime.

Q1. Show that $P = (x_1, y_1)$ has order 3 if an only if $2P = -P$. Use this fact to prove that if $P = (x_1, y_1)$ has order 3 then

$$3x_1^4 + 6ax_1^2 + 12x_1b - a^2 = 0$$

Q2. Show that there are at most 8 points of order 3 on this curve E.

Q3. Let $p = 73, a = 43, b = 0$. Find all points of order 3 (brute force not allowed).

Some code fragments which might help, actually Q1 is solved BEST by paper and pencil maths!!! Q3 is solved best by actually solving a polynomial equation.

```
E = EllipticCurve(GF(7), [1,6]); E.cardinality()
[ E.random_point().order() for n in range(1,10) ]
```

```
(X,Y) = E.multiplication_by_m(3); X
[ (29*(E.random_point())).order() for n in range(1,10) ]
```

5.1. Finding Roots over Finite Fields to solve Q3

Some very nice methods:

```
P.<x> = PolynomialRing(K, implementation='NTL')
f = 3*x^4 + 6*43*x^2 - 43^2 ???
f.roots(multiplicities=False)
f.small_roots()
```

another very nice method by James Carlson, needs some adaptations to mod p case

```
def qq2zz(f):
 # clear denominators of f
 c = f.coeffs()
 d = map( lambda g: g.denom(), c)
 return lcm(d)*f

def roots(f, q):
# return list of roots of f in finite field of q elements
K.<T> = GF(q)
r = [ ]
```

```
g = qq2zz(f).change_ring(K)
for a in K:
if g(a) == 0:
r.append(a)
return r

def search(f,a,b,k):
 # search for roots of f in GF(p^k) for p in [a,b]
  for p in prime_range(a,b):
   rr = roots(f,p^k)
   if rr != [ ]:
    print p, rr
S.<u> = PolynomialRing(QQ)
f = 2/5*u^5 + 3/7*u^2 + 1
search(f, 2, 20, 2)
```

Roots with 2 variables a and b? Possible, one method is to use resultants, we will post sample code later. (see code in our last year project TwinFace).

Solutions to Exercises

Exercise 1(b) If $P \neq Q$, we set $s = (y_1 - y_2)(x_1 - x_2)^{-1}$. If $P = Q$, we take $s = (3x_1^2 + a)(2y_1)^{-1}$. Then, $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$, where $x_3 = s^2 - x_1 - x_2$, and $y_3 = s(x_1 - x_3) - y_1$.

These formulae come from the definition of addition on an elliptic curve that you saw in the video. This uses different points of intersection between straight lines and the curve. $\square$

Exercise 1(c) Substituting the coordinates of P into the correct formula from the previous part shows that $2^*P = Q$. $\square$

Exercise 1(d) You should find that $P + Q = (1, 0)$. $\square$