CS 161 – Computer Security
Instructor: Tygar
29 September 2014

Homework 3 Answer Set

Notes

- Homework 3 is due on 29 September 2015 at 3PM.
- Please work on this homework individually – no collaboration allowed.
- Please submit this homework in PDF format.
- It is possible to answer all questions relatively briefly. Please limit your answer to each question to a page at most.
- Submit this homework using Gradescope.

Please start the answer to each question on a new page

For the following questions, please consider the elliptic curve : $y^2 = x^3 + 4x + 3$. You may use any computational tools you wish (except receiving help from another human) for the following questions. Please list any computational tools you use.

However, we recommend attempting as much of this problem set by hand as possible: you will likely have midterm questions which require you to compute similar values by hand.

1. List the points of the $E \bmod p$ for $p = 3, 5, 7, 11, 13$

$p = 3$: $\mathcal{O}$, (0,0), (2,1), (2,2)
$p = 5$: $\mathcal{O}$, (2,2), (2,3)
$p = 7$: $\mathcal{O}$, (1,1), (1,6), (3,0), (5,1), (5,6)
$p = 11$: $\mathcal{O}$, (0,5), (0,6), (3,3), (3,8), (5,4), (5,7), (6,1), (6,10), (7,0), (9,3), (9,8), (10,3), (10,8)
$p = 13$: $\mathcal{O}$, (0,4), (0,9), (3,4), (3,9), (6,3), (6,10), (7,6), (7,7), (8,1), (8,12), (9,1), (9,12), (10,4), (10,9), (11,0)

2. For each of the above cases compute the trace of Frobenius $t_p = p + 1 - (\#\text{ of points in } E)$ and verify that $|t_p| < 2\sqrt{p}$.

p	# of points in E	t_p	$2\sqrt{p}$
3	4	0	3.46
5	3	3	4.47
7	6	2	5.29
11	14	-2	6.63
13	16	-2	7.21

3. Write the addition table for $E \bmod 7$

	$\mathcal{O}$	(1,1)	(1,6)	(3,0)	(5,1)	(5,6)
$\mathcal{O}$	$\mathcal{O}$	(1,1)	(1,6)	(3,0)	(5,1)	(5,6)
(1,1)	(1,1)	(5,6)	$\mathcal{O}$	(5,1)	(1,6)	(3,0)
(1,6)	(1,6)	$\mathcal{O}$	(5,1)	(5,6)	(3,0)	(1,1)
(3,0)	(3,0)	(5,1)	(5,6)	$\mathcal{O}$	(1,1)	(1,6)
(5,1)	(5,1)	(1,6)	(3,0)	(1,1)	(5,6)	$\mathcal{O}$
(5,6)	(5,6)	(3,0)	(1,1)	(1,6)	$\mathcal{O}$	(5,1)

APPENDIX: Here is a Sage worksheet (you can run at https://cloud.sagemath.com/) that solves this homework. However, I hope everyone did this homework by hand – because this homework is exactly the sort of question I might ask on a midterm when no calculator is available.

```
# This Sage worksheet solves CS 161 Fall 2015 HW3
#
# Function str_ell_pt takes an elliptic curve point s in projective form and converts
# to a string (including "point at infinity")
def str_ell_pt(x):
    if x[2]==0:
        return "point at infinity"
    elif x[2]==1:
        return "(" + str(x[0]) + "," + str(x[1])+")"
    else:
        return "error"

# Function str_points takes an elliptic curve and produces a string containing
# the list of points in the curve
def str_points(x):
    s=""
    first = true
    for i in x.points():
        if not first:
            s += ", "
        s += str_ell_pt(i)
        first = false
    return s

# This constructor creates a dictionary "curves" for y^2 = x^3 + 4*x + 3 modulo p for
# p = 3, 5, 7, 11, 13
curves = {p:EllipticCurve(GF(p),[4,3]) for p in (3, 5,7,11,13)}

print "HW 3.1"
for i in sorted(curves):
    print "E mod", i, "has points:", str_points(curves[i])
print

print "HW 3.2"
for i in sorted(curves):
     print "For p =", i, ": E has", curves[i].order(),
     print "points & trace of Frobenius =", curves[i].trace_of_frobenius(),
     print "but 2*sqrt("+str(i)+") =", "%.2f"%(2.0*(i^0.5))
print

print "HW 3.3"
print "Here is the addition table over the", curves[7]
for i in curves[7]:
    for j in curves [7]:
        print str_ell_pt(i), "+", str_ell_pt(j), "=", str_ell_pt(i+j)
```