Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 10

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, January 12th, at 12:05 pm.

1. Show that each of the following elliptic curves over $\mathbb{Q}$ has the stated torsion group $E(\mathbb{Q})_{\text{tors}}$:

(a) $y^2 = x^3 - x$; $\quad \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

(b) $y^2 = x^3 + 1$; $\quad \mathbb{Z}_6$.

2. Let E be the curve $y^2 = x^3 + 2x + 1$ over the field $\mathbb{F}_7$. Prove that this curve is elliptic (i.e., nonsingular) and that $E(\mathbb{F}_7) \cong \mathbb{Z}_5$. Choose a generator g of $E(\mathbb{F}_7)$ and write each element of this group as kg for some k. Do not forget that $\mathcal{O} \in E(\mathbb{F}_7)$.

3. Let E_c be the elliptic curve given by $y^2 = x^3 + 2x + c$ over the field $\mathbb{F}_7$. Find a parameter c so that

(a) $\#E_c(\mathbb{F}_7) = 6$,

(b) $\#E_c(\mathbb{F}_7) = 8$.

Are these groups cyclic?

4. Let E_b be the elliptic curve $y^2 = x^3 + bx + 1$ over the field $\mathbb{F}_7$. Make a list of all possible groups $E_b(\mathbb{F}_7)$ giving their elements (points) and showing their structure (in terms of groups $\mathbb{Z}_n$ or their direct sums). In each case verify that

$$|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$$

(Hasse's theorem).

I wish you a merry Christmas and a happy New Year!