Lecture 12

Jose Capco (jcapco@risc.jku.at)

Henceforth, in this course, we will focus our attention only on elliptic curves (mostly over $\mathbb{Q}$).

In ECM, understanding the torsion points of a curve is of interest. Because, for a prime $p \mid n$, we want to find a $P \in G_n$ we hope that P is a β-torsion point (i.e. $\beta P = O$). We start first our investigation of the torsion points from an algebraically-closed perspective. Define for $n \in \mathbb{N}$

$$E[n] := \{P \in E(\bar{K}) \,:\, nP = O\}$$

clearly $E[n]$ is a subgroup of $E(\bar{K})$ called the *n-torsion points of* $E(\bar{K})$[1]. But we will also see that $E[n]$ is a finite abelian group. The notation is used for any group

Notation. If n is any natural number and G is a (additive) group then we denote its n-torsion subgroup as

$$G[n] := \{g \in G \,:\, ng = 0\}$$

Example 1. Consider an elliptic curve $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ (Legendre form) with e_i distinct (not necessarily in K, but in $\bar{K}$). It is easy to compute the 2-torsion points of $E(\bar{K})$ they are

$$\{O, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

and it is easy to see that this is group-isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Let us divert a little bit and recall some facts in Group Theory ...

Definition. Let G be a finite abelian group and p a prime number dividing $\#G$

- G is called a *p-group* if $\#G = p^k$ for some $k \in \mathbb{N}$
- Let us temporarily, for this session, denote the maximum p-subgroup of G as

  $$G_p := \bigcup_{i=k}^{\infty} G[p^k]$$

  this is also called the *Sylow p-subgroup* of G or (esp. for finite abelian case) the *primary p-subgroup* of G.

Theorem 2. Let G be a finite abelian group then

1. (Fundamental Theorem of Finite Abelian Groups. FTFAG.) G is a direct sum of cyclic groups with prime power order. Two finite abelian groups are isomorphic iff these prime powers expressed as ordered tuples are the same.
2. (Basis Theorem) G is a direct sum of cyclic groups.
3. (Structure Theorem) G is a direct sum of cyclic groups with (unique) *invariant factors*[2] i.e.

   $$G \cong \mathbb{Z}/d_1 \oplus \mathbb{Z}/d_2 \oplus \mathbb{Z}/d_3 \cdots \oplus \mathbb{Z}/d_k$$

   where $d_i \mid d_{i+1}$ for $i = 1, \ldots, k-1$. Two finite abelian groups are isomorphic iff their invariant factors expressed as ordered $\mathbb{N}$-tuples are the same.

[1] in some literatures $E[n]$ involve only K-rational points. This will be explained once we discuss torsion subgroups of E.

[2] also called *canonical decomposition*

Proof Idea. Clearly, the Basis Theorem follows immediately from FTFAG. To prove FTFAG One first show that this is true for abelian groups that are p-groups. So if G is a p-group then one can find (by Cauchy, since this has a subgroup isomorphic to $\mathbb{Z}/p$) a non-trivial maximum cyclic subgroup C and another proper subgroup H such that

$$G = C \oplus H$$

Applying this recursively proves FTFAG for p-groups. One then shows the *Primary Decomposition for Finite Abelian Groups*, i.e. a finite abelain group is the direct sum of its maximum p-subgroups, i.e. for arbitrary finite abelian group G we have

$$G = \bigoplus_{p \mid \# G} G_p$$

Decomposing these maximal p-subgroups will then give FTFAG for arbitrary finite abelian group G.

Structure Theorem follows from re-ordering the cyclic p-groups in the decomposition of G (for different primes p dividing $\#G$) and using the Chinese Remainder Theorem. This last step is best shown by an example. □

Example 3. Suppose we have decomposed G into cyclic groups of prime power order, e.g. let G be

$$G = (\mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/16) \oplus (\mathbb{Z}/3 \oplus \mathbb{Z}/9)$$

1. We write the prime power decompositions in increasing order as above.
2. Suppose $p_1, \ldots, p_n$ are the prime numbers dividing $\#G$, in this case $n = 2$.
3. We get the number k that is the greatest number of decomposition of the maximal p-subgroups of G, in this case $k = 3$ since the maximum 2-subgroups has 3 decompositions.
4. Now we write k n-tuples in decreasing lexicographic order starting from the maximum prime powers (use 0 if the prime decompositions are exhausted). So for this particular example we have
$$(16, 9) > (4, 3) > (2, 0)$$
5. Finally we write the canonical decomposition in that order using chinese remainder theorem
$$G = (\mathbb{Z}/2) \oplus (\mathbb{Z}/4 \oplus \mathbb{Z}/3) \oplus (\mathbb{Z}/16 \oplus \mathbb{Z}/9) = \mathbb{Z}/2 \oplus \mathbb{Z}/12 \oplus \mathbb{Z}/144$$

Exercise 1. If we identify finite abelian groups up to isomorphisms, how many finite abelian groups are there that have order $n \in \mathbb{N}$? (Hint: Research partition numbers).

Remark 4. An easy consequence of Structure Theorem is that for a finite abelian group G, a prime number p and a positive integer $k \in \mathbb{N}$:

$$G[p] \text{ is cyclic } \Leftrightarrow G[p^k] \text{ is cyclic}$$

Now we can show that for any field K the n-torsion points are finite, in particular ...

Theorem 5. Let $p = \operatorname{char} K$ ad suppose that E is an elliptic curve and $n \in \mathbb{N}$ and write $n = p^r m$ where $p^r \mid\mid n$. Then either $E[n] \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$ or $E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$. The latter case always holds for $p \nmid n$ (spec. if $p = 0$).

Proof. Clearly for any elliptic curve E over some field K, the n-torsion subgroup is a finite abelian group since $E[n] = \ker[n]$ and we know from the last lectures that $\# \ker[n] \leq n^2$. Thus $E[n]$ is indeed a finite abelian group. We now consider two cases

Case $p \nmid n$: We know from last lectures that this implies that the isogeny $[n]$ is separable and this implies (again from the last lectures) that $\#\ker[n] = \deg[n] = n^2$. We then use the Structure Theorem for finite abelian groups:

$$E[n] \cong \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \cdots \oplus \mathbb{Z}/n_k \qquad n_i \mid n_{i+1}$$

If l is a prime divisor of n_1 then $E[l] \geq E[n]$ and since $l \mid n_i$ for all i, we get

$$\#(\bigoplus_{i=1}^{k} \mathbb{Z}/n_i)[l] = \#\bigoplus_{i=1}^{k}(\mathbb{Z}/n_i)[l] = \prod_{i=1}^{k} l = l^k$$

So $\#E[l] = l^k$, but we know (similar to $E[n]$) beforehand that $\#E[l] = l^2$ which implies that $k = 2$ and so

$$E[n] \cong \mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2 \qquad n_1 \mid n_2$$

so this implies that $\#E[n] = n_1 n_2 = n^2$ which implies that $n_1 = n_2 = n$ (n_1 and n_2 both divide n because $(1,0)$ has order n_1 and $(0,1)$ has order n_2. By definition of $E[n]$, $n(1,0) = n(0,1) = (0,0)$).

Case $p \mid n$: From the last lecture we know that in this case $[n]$ is not separable and

$$\#E[n] = \#\ker[n] < \deg[n]$$

thus $E[n]$ is again a finite abelian group. We know by primary decomposition of finite abelian groups that

$$E[n] = E[p^r] \oplus E[m]$$

Therefore, it suffices to determine $E[p^r]$ (since $E[m]$ is the previous case). Now $E[p] < p^2$ and is a p-group so it must be either isomorphic to $\mathbb{Z}/p$ or the trivial froup 0.

If $E[p]$ is trivial then for any $k \in \mathbb{N}$ and $P \in E[p^k]$, if P has order p^l with $l > 1$ then $p^{l-1}P$ has order p which can only be O, so P can only be O. Thus, $E[p]$ is trivial iff $E[p^k]$ is trivial for any $k \in \mathbb{N}$. In this case,

$$E[n] = E[m] \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$$

Now suppose that $E[p]$ is non-trivial, thus $E[p^k]$ is non-trivial and cyclic for any $k \in \mathbb{N}$ (see Remark 4). We want to show that $E[p^k]$ is isomorphic to $\mathbb{Z}/p^k$ for any $k \in \mathbb{N}$. So it suffices to show that E has a point of order p^k (and since $E[p^k]$ is cyclic this amounts to $E[p^k] \cong \mathbb{Z}/p^k$. Recall that the isogeny $[p]$ is non-constant (otherwise its kernel would be infinite), so $[p]$ is surjective. Suppose $P_1 \in E(\bar{K})$ has order p, then we can find a preimage $P_2 \in [p]^{-1}(P_1)$ i.e. $pP_2 = P_1$ and $p^2 P_2 = O$ so P_2 has order p^2. Iterating this procedure will give us a $P_k \in E(\bar{K})$ of order p^k. Thus, in this particular case

$$E[n] \cong E[m] \oplus E[p^r] \cong \mathbb{Z}/m \oplus (\mathbb{Z}/m \oplus \mathbb{Z}/p^r) \cong \mathbb{Z}/m \oplus \mathbb{Z}/n$$

□

Let G be an abelian group, then the *torsion subgroup* of G is a subgroup defined and denoted as

$$\mathrm{Tor}(G) := \bigcup_{n \in \mathbb{N}} G[n]$$

The torsion subgroup of an abelian group is not necessarily finite. This is also true for elliptic curves. For instance any elliptic curve over $\mathbb{C}$ (as we have seen in the introductory part) is isomorphic to a torus i.e. a group $\mathbb{C}/L$ for some lattice $L \leq (\mathbb{C}, +)$, and this has clearly a torsion subgroup with infinite number of elements. However, the beautiful surprise is that if E is any elliptic curve over $\mathbb{Q}$ then $\#\,\mathrm{Tor}(E) < \infty$, here we should be aware of a subtle point here: When dealing with $E[n]$ we work consider $\overline{\mathbb{Q}}$-rational points, while when dealing with $\mathrm{Tor}(E)$ we deal with $\mathbb{Q}$-rational points i.e. for us $\mathrm{Tor}(E(K))$ is

$$\mathrm{Tor}(E) := \{P \in E(K) : \exists n \in \mathbb{N} \ni nP = O\}$$

this is the reason why our $E[n]$ is sometimes more precisely denoted as $E(\bar{K})[n]$ while $E[n]$ itself involves only K-rational points. Naturally, our Theorem 5 on the structure of $E[n]$ holds for $\bar{K}$-rational points.

The finiteness of $\mathrm{Tor}(E(\mathbb{Q}))$ is a corollary of the celebrated Nagell-Lutz[3] Theorem.

Notation. We sometimes adapt the common notation E/K to mean that E is an elliptic curve over K.

Nagell-Lutz Theorem. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ defined in such a way that $a, b \in \mathbb{Z}$ and suppose $\Delta := 4a^3 + 27b^2$ is its discriminant. The non-trivial torsion points of E are points $P \in \mathbb{A}^2(\mathbb{Q})$ $(P = (x_P, y_P))$ satisfying

1. $x_P, y_P \in \mathbb{Z}$
2. If $y_P \neq 0$ then $y_P^2 \mid \Delta$

Example 6. Consider the elliptic curve $E/\mathbb{Q} : y^2 = x^3 + 1$. We can use Nagell-Lutz to determine the torsion subgroup of E. The discriminant is $\Delta = 27$ and the divisors are $(\pm 1)^2, (\pm 3)^2$, so the candidate y-coordinates are

$$y = 0, \pm 1, \pm 3$$

If $y = 0$ then only $x = -1$ satisfy the equation, and in this case we have the only non-trivial 2-torsion point $(-1, 0)$. The points with $y = \pm 1$ are $(0, \pm 1)$, it suffices to check that $P = (0, 1)$ is a torsion point (because $\mathrm{Tor}(E)$ is a subgroup of E and $-P = (0, -1)$). One checks that $3P = O$, so indeed $(0, \pm 1)$ are 3-torsion points. The points with $y = \pm 3$ are $(2, \pm 3)$, again it suffices to check if $(2, 3)$ is a torsion point. Recall that $Q = (-1, 0)$ is a 2-torision point and one checks that $P + Q = (2, 3)$ and because $\mathrm{Tor}(E)$ is a subgroup, we learn that $(2, \pm 3)$ is a torsion point. In fact, $E \cong \mathbb{Z}/6$.

[3]we write the names in chronological order of the publications that is associated to the theorem