3.2 Division Polynomials

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
1. Goal

2. Define division polynomials $\psi_m$

3. Define division polynomials $\phi_m$ and $\omega_m$

4. Theorem 3.6 and Corollary 3.7

5. Group structure of n-torsion group
   - $p \nmid n$
   - $p \mid n$
   - Conclusion
Goal

- The goal of this section is:
  1. to prove Theorem 3.2
  2. needed in Section 4.2
Define division polynomials $\psi_m$

- Define division polynomials $\psi_m \in \mathbb{Z}[x, y, A, B]$
  
  $\psi_0 = 0$
  $\psi_1 = 1$
  $\psi_2 = 2y$
  $\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
  $\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
  $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_m^{-1}\psi_{m+1}^3$ for $m \geq 2$
  $\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ for $m \geq 3$

Lemma 3.3

- $\psi_n \in \mathbb{Z}[x, y^2, A, B]$  $n$: odd
- $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$  $n$: even
Define division polynomials $\phi_m$ and $\omega_m$

- Define:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$$
$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1} - \psi_{m-2}\psi_{m+1})$$

**Lemma 3.4**

$$\phi_n \in \mathbb{Z}[x, y^2, A, B] \quad \forall n$$
$$\omega_n \in y\mathbb{Z}[x, y^2, A, B] \quad n: \text{odd}$$
$$\omega_n \in \mathbb{Z}[x, y^2, A, B] \quad n: \text{even}$$

$\therefore \mathbb{Z}[x, y^2, A, B] \rightarrow \mathbb{Z}[x, A, B]$
$\therefore \phi_n, \psi_n^2 \text{ always a polynomial in } x$
(but $\psi_n$ is not necessarily a polynomial in $x$)
Lemma 3.5

\[ \phi_n(x) = x^{n^2} + \text{lower degree terms} \]
\[ \psi^2_n(x) = n^2 x^{n^2-1} + \text{lower degree terms} \]
Theorem 3.6 and Corollary 3.7

**Theorem 3.6**

\[ P = (x, y) \text{ on } y^2 = x^3 + Ax + B , \text{ char.}(K) \neq 2 . \text{ Then} \]

\[ nP = \left( \frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right) \]

Proof will be given in Section 9.5.

**Corollary 3.7**

*Endomorphism* \( \alpha : P \mapsto nP , \deg(\alpha) = n^2 \)

Proof:

\[ r(x) = \frac{\phi_n(x)}{\psi_n^2(x)} , \quad \phi_n, \psi_n^2 \text{ has no common roots.} \]
For $p \nmid n$, $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$

Proof:

- $E[n]$: kernel of $\alpha$
  - $\# \text{ kernel of } \alpha = \deg(\alpha)$
  - $\because \alpha$ is separable, $\therefore \#E[n] = \deg(\alpha) = n^2$

- By Appendix B
  The structure theorem for finite abelian groups:
  
  $$E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$
  for some $n_1, n_2, \cdots, n_k$ with $n_i \mid n_{i+1}$

- Let $l$ be a prime with $l \mid n_1$, then $l \mid n_i$
  $\rightarrow E[l] \subseteq E[n]$, so $E[n]$ has order $l^k$

Since $\#E[l] = l^2$, $\therefore k = 2$

$\therefore E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$
For $p | n$

- By Proposition 2.27, $\alpha(P) = pP$ is not separable
  $\Rightarrow \#E[p] < \deg(\alpha) = p^2$
  $\therefore \#E[p] = 1 \text{ or } p$

- If $\#E[p] = 1$ then $\#E[p^k] = 1$

- Suppose $\#E[p] = p$, we claim $E[p^k] \simeq \mathbb{Z}_{p^k}$

  **Proof:**
  1. easy to see $E[p^k]$ is cyclic
  2. $E[p^k]$ is cyclic of order $p^k$

  Suppose $\exists$ an element $P$ of order $p^j$

  By Theorem 2.21, multiplication by $p$ is surjective
  so $\exists$ point $Q$ such that $pQ = P$

  $\rightarrow p^jQ = p^{j-1}P \neq \infty$ but $p^{j+1}Q = p^jP = \infty$

  $\therefore Q$ has order $p^{j+1}$.

  By induction, there are points of order $p^k$ for all $k$
Group structure of $E[n]$

- Now put everything together.

Write $n = p^r n'$ with $r \geq 0, \ p \nmid n'$

Then

$$E[n] \simeq E[n'] \oplus E[p^r]$$

We have $E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ and we just showed that $E[p^r] \simeq 0$ or $\mathbb{Z}_{p^r}$

Recall that $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \simeq \mathbb{Z}_{n'p^r} = \mathbb{Z}_n$

So we have

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ or } \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$