Combinatorial Aspects of Elliptic Curves over Finite Fields

Gregg Musiker

University of California, San Diego

FPSAC 2006

June 19, 2006

OUTLINE

I. Introduction

II. A Combinatorial Interpretation of N_k

III. Understanding Number Theoretically

$$N_2 = (2 + 2q)N_1 - N_1^2$$

IV. A Geometric Interpretation of N_k

I. INTRODUCTION

A model for a **Hyperelliptic Curve** (with a rational point) is an equation of the form

$$y^2 = f(x)$$

where $f(x)$ is a polynomial of degree $2g+1$ with all roots distinct, and coefficients in a field K of characteristic $\neq 2$.

We will let C denote the zero locus of such a curve with $(x, y)-$coordinates in K.

Projectivizing, we also obtain one point at infinity P_∞.

The number g is a positive integer known as the **genus** of the curve.

We let K be $\mathbb{F}_q$, a finite field containing q elements, where q is a power of a prime.

We can also let K be a field extension of $\mathbb{F}_q$, such as $\mathbb{F}_{q^k}$, or even the algebraic closure $\overline{\mathbb{F}_q}$.

$C(\mathbb{F}_q)$, $C(\mathbb{F}_{q^k})$, or $C(\overline{\mathbb{F}_q})$ will denote the curves over these fields, respectively.

$$C(\mathbb{F}_q) \subset C(\mathbb{F}_{q^{k_1}}) \subset C(\mathbb{F}_{q^{k_2}}) \subset \cdots \subset C(\overline{\mathbb{F}_q})$$

for any sequence of natural numbers $1|k_1|k_2| \ldots$.

The Frobenius automorphism π acts on curve C over finite field $\mathbb{F}_q$ via

$$\pi(a, b) = (a^q, b^q).$$

Fact 1 *For a point* $P \in C(\overline{\mathbb{F}_q})$,

$$\pi(P) \in C(\overline{\mathbb{F}_q}).$$

Fact 2 *For a point* $P \in C(\mathbb{F}_{q^k})$,

$$\pi^k(P) = P.$$

Let N_m signify the number of points on curve C, over finite field $\mathbb{F}_{q^m}$.

Alternatively, N_m counts the number of points in $C(\overline{\mathbb{F}_q})$ which are fixed by the mth power of the Frobenius automorphism, π^m.

Using this sequence, we define the **Zeta Function** as the exponential generating function.

$$Z(C,T) \quad = \quad \exp\left(\sum_{m=1}^{\infty} N_m \frac{T^m}{m}\right)$$

Theorem 1 (Rationality - Weil 1948)

$$Z(C,T) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)\cdots(1-\alpha_{2g-1}T)(1-\alpha_{2g}T)}{(1-T)(1-qT)}$$

for complex numbers α_i's, where g is the genus of the curve C. Furthermore, the numerator of $Z(C,T)$, which we will denote as $L(C,T)$, has integer coefficients.

Theorem 2 (Functional Equation - Weil 1948)

$$Z(C,T) = q^{g-1}T^{2g-2}Z(C,1/qT)$$

As a corollary to Rationality we get

$$\begin{aligned} N_k &= p_k[1 + q - \alpha_1 - \cdots - \alpha_{2g}] \\ &= 1 + q^k - \alpha_1^k - \cdots - \alpha_{2g}^k \end{aligned}$$

and the Functional Equation implies up to permutation,

$$\alpha_{2i-1}\alpha_{2i} = q.$$

By Rationality and the Functional Equation:

The Zeta Function of curve C of genus g,

hence the entire sequence of $\{N_k\}$'s,

only depends on $\{q, N_1, N_2, \ldots, N_g\}$.

Specializing to the case of an elliptic curve E, where $g = 1$, a lot more is known and there is additional structure.

Fact 3 *E can be represented as the zero locus in $\mathbb{P}^2$ of the equation*

$$y^2 = x^3 + Ax + B$$

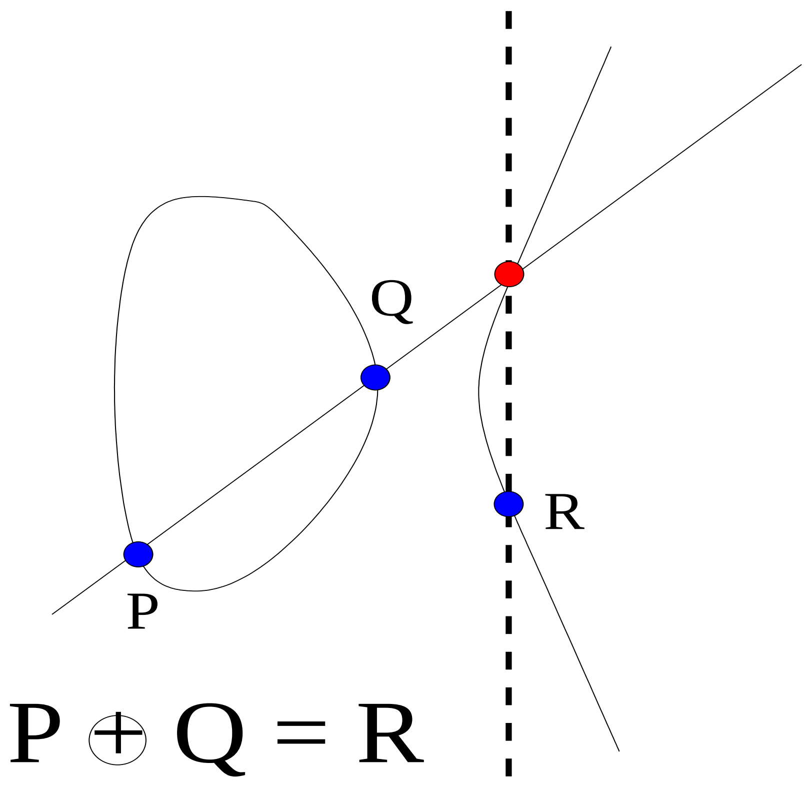
for $A, B \in \mathbb{F}_q$. (if $p \neq 2,\ 3$)

Fact 4 *E has a group structure where two points on E can be added to yield another point on the curve.*

Fact 5 *The Frobenius automorphism is compatible with the group structure:*

$$\pi(P \oplus Q) = \pi(P) \oplus \pi(Q).$$

Draw Chord/Tangent Line and then reflect about horizontal axis



If $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, then

$$P_1 \oplus P_2 = P_3 = (x_3, y_3) \text{ where}$$

1) If $x_1 \neq x_2$ then

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = m(x_1 - x_3) - y_1 \text{ with } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2) If $x_1 = x_2$ but ($y_1 \neq y_2$, or $y_1 = 0 = y_2$) then $P_3 = P_\infty$.

3) If $P_1 = P_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1 \text{ and } y_3 = m(x_1 - x_3) - y_1 \text{ with } m = \frac{3x_1^2 + A}{2y_1}.$$

4) P_∞ acts as the identity element in this addition.

Theorem 3 (Garsia ? 2004) *For an elliptic curve, we can write N_k as a polynomial in terms of N_1 and q such that*

$$N_k = \sum_{i=1}^{k} (-1)^{i-1} P_{k,i}(q) N_1^i$$

where each $P_{k,i}$ is a polynomial in q with positive integer coefficients.

This can be proven using the fact that

$$N_k = 1 + q^k - \alpha_1^k - \alpha_2^k$$

and this leads to a recursion for $\alpha_1^k + \alpha_2^k$ in terms of

$$\begin{aligned} \alpha_1 + \alpha_2 &= 1 + q - N_1 \quad \text{and} \\ \alpha_1 \alpha_2 &= q. \end{aligned}$$

We can prove positivity by induction.

$$
\begin{aligned}
N_2 &= (2+2q)N_1 - N_1^2 \\
N_3 &= (3+3q+3q^2)N_1 - (3+3q)N_1^2 + N_1^3 \\
N_4 &= (4+4q+4q^2+4q^3)N_1 - (6+8q+6q^2)N_1^2 + (4+4q)N_1^3 - N_1^4 \\
N_5 &= (5+5q+5q^2+5q^3+5q^4)N_1 - (10+15q+15q^2+10q^3)N_1^2 \\
&+ (10+15q+10q^2)N_1^3 - (5+5q)N_1^4 + N_1^5
\end{aligned}
$$

Question 1 *What is a combinatorial interpretation of these expressions, i.e. of the* $P_{k,i}$*'s?*

II. A COMBINATORIAL INTERPRETATION OF N_k.

Fibonacci Numbers

$$F_n = F_{n-1} + F_{n-2}$$

$$F_0 = 1, \quad F_1 = 1$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34 \ldots$$

Counts the number of subsets of $\{1, 2, \ldots, n-1\}$ with no two elements consecutive

e.g. $F_5 = 8 : \quad \{\ \},\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\},\ \{1,4\},\ \{2,4\}$

Lucas Numbers

$$L_n = L_{n-1} + L_{n-2}$$

$$L_1 = 1, \quad L_2 = 3$$

$$1, 3, 4, 7, 11, 18, 29, 47, \ldots$$

Counts the number of subsets of $\{1, 2, \ldots, \mathbf{n}\}$ with no two elements **circularly** consecutive

e.g. $L_4 = 7 :$ $\{\ \},\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\},\qquad \{2,4\}$

By Convention and Recurrence: $L_0 = 2$

Definition 1 *We define the* $(\mathbf{q},\mathbf{t})-$**Lucas numbers** *to be a sequence of polynomials in variables* q *and* t *such that* $L_n(q,t)$ *is defined as*

$$L_n(q,t) = \sum_S q^{\#\text{ even elements in } S}\; t^{\lfloor \frac{n}{2} \rfloor - \#S}$$

where the sum is over subsets S *of* $\{1,2,\ldots,n\}$ *such that no two numbers are circularly consecutive.*

e.g. $L_2 = 3: \quad \{\ \},\ \{1\},\ \{2\}$

$L_2(q,t) = \ q^0t^1 + q^0t^0 + q^1t^0 = 1 + q + t$

e.g. $L_4 = 7: \quad \{\ \},\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{1,3\}, \qquad \{2,4\}$

$$\begin{aligned} L_4(q,t) = &\ q^0t^2 + q^0t^1 + q^1t^1 + q^0t^1 + q^1t^1 + q^0t^0 \quad + \quad q^2t^0 \\ = &\ 1 + q^2 + (2q+2)t + t^2 \end{aligned}$$

Theorem 4 (M- 2005)

$$L_{2k}(q,t) = 1 + q^k - N_k\Big|_{N_1=-t}$$

We prove this by showing that the left- and right-hand-sides satisfy the same initial conditions and recurrence relations:

$$\begin{aligned} L_2(q,t) &= 1 + q + t \\ L_4(q,t) &= 1 + q^2 + (2+2q)t + t^2 \end{aligned}$$

The $L_{2k}(q,t)$'s satisfy recurrence relation

$$L_{2k+2}(q,t) = (1+q+t)L_{2k}(q,t) - qL_{2k-2}(q,t).$$

The right-hand-sides are equal to $1 + q^k - N_k\Big|_{N_1=-t} = \alpha_1^k + \alpha_2^k$

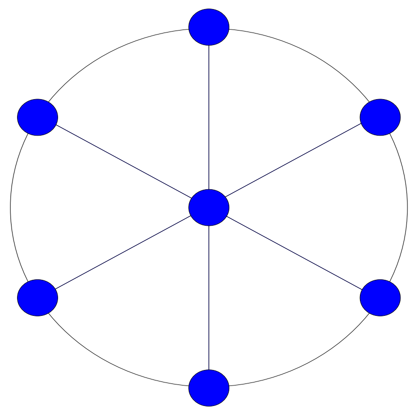
$$\alpha_1^{k+1} + \alpha_2^{k+1} = (1+q-N_1)(\alpha_1^k + \alpha_2^k) - q(\alpha_1^{k-1} + \alpha_2^{k-1})$$

Question 2 *Is there a generating function equal to N_k directly?*

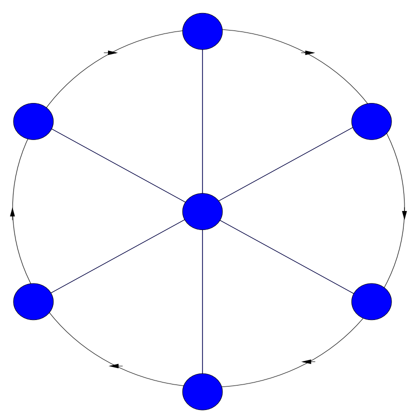
Question 2 *Is there a generating function equal to N_k directly?*

We can come close.

We let W_n denote the wheel graph which consists of n vertices on a circle and a central vertex which is adjacent to every other vertex.



We let W_n denote the wheel graph which consists of n vertices on a circle and a central vertex which is adjacent to every other vertex.



We note that a spanning tree will consist of arcs on the rim and spokes. We orient the arcs clockwise and designate the head of each arc.

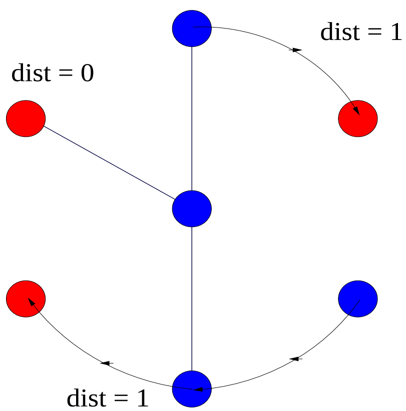
Definition 2

$$\mathcal{W}_k(q,t) = \sum_{\text{spanning trees of } W_k} q^{\text{total dist from spokes to tails}}\, t^{\#\text{ spokes}}.$$

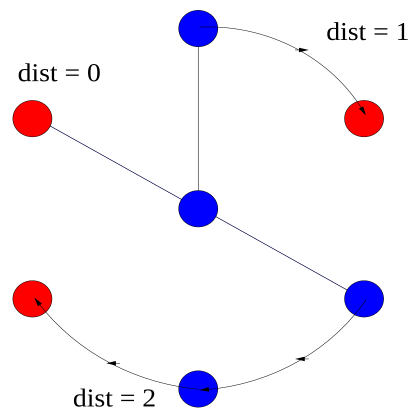
Theorem 5 (M- 2005)

$$\mathcal{W}_k(q,t) = -N_k\big|_{N_1=-t} = \sum_{i=1}^{k} P_{k,i}(q)\ t^i \quad \text{for all } k \geq 1.$$

q^2t^3



q^3t^3



The proof uses combinatorial facts from [Egecioglu-Remmel 1990] and [Benjamin-Yerger 2004].

Number Theoretic Interpretation of $N_k(q, N_1)$'s?

Algebraic Geometric Interpretation of $N_k(q, N_1)$'s?

IV. UNDERSTANDING NUMBER THEORETICALLY

$$N_2 = (2 + 2q)N_1 - N_1^2.$$

Our first observation is the factorization:

$$N_2 = N_1 \cdot (2 + 2q - N_1).$$

N_1 clearly counts objects, namely points on elliptic curve E.

Does the second factor also count something?

Our first observation is the factorization:

$$N_2 = N_1 \cdot (2 + 2q - N_1).$$

N_1 clearly counts objects, namely points on elliptic curve E.

Does the second factor also count something?

YES,

$2 + 2q - N_1$ counts the number of points on E^t.

If E has equation (char $\neq 2,\ 3$)

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

then E^t has equation $y^2 = x^3 + a\Lambda^{-2}x + b\Lambda^{-3}$ for $\Lambda \neq \alpha^2,\ \alpha \in \mathbb{F}_q$.

The isomorphism class of E^t doesn't depend on the choice of Λ, as long as it is a non-square, and

$$E^t : \quad y^2 = x^3 + a\Lambda^{-2}x + b\Lambda^{-3}$$

is also isomorphic to the curve with equation

$$y^2 = \Lambda \cdot (x^3 + ax + b).$$

E^t also isomorphic to $E'(\mathbb{F}_q) \leq E(\mathbb{F}_{q^2})$,

the set

$$\left\{(\alpha, \lambda\beta) \in E(\mathbb{F}_{q^2}) : \alpha, \beta \in \mathbb{F}_q, \quad \lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q\right\}$$

We follow [Stark 1973] and partition the set $\mathbb{F}_q$ into three sets:

We let $\mathcal{I}_1$ denote the number of $\alpha \in \mathbb{F}_q$ such that α is the $x-$coordinate of some ordinary point on E, i.e. $(\alpha, \beta),\ \beta \neq 0$.

We let $\mathcal{I}_0$ denote the number of $\alpha \in \mathbb{F}_q$ such that α is the $x-$coordinate of a special point on E, i.e. $(\alpha, 0)$.

We let $\mathcal{I}_{-1}$ denote the number of $\alpha \in \mathbb{F}_q$ such that α is **not** the $x-$coordinate of some point on E.

If the equation of E is $y^2 = f(x)$, these can also be described as:

$$\mathcal{I}_i = \#\{\alpha \in \mathbb{F}_q \text{ such that } f(\alpha)^{\frac{q-1}{2}} = i\}$$

Since these three possibilities partition the set $\mathbb{F}_q$, we obtain

$$\mathcal{I}_{-1} + \mathcal{I}_0 + \mathcal{I}_1 = q.$$

Since ordinary points come in conjugate pairs, and special and infinite points come singleton, we get futher

$$N_1(E) = 2\mathcal{I}_1 + \mathcal{I}_0 + 1.$$

Lastly, by the definition of E^t, we conclude

$$N_1(E^t) = 2\mathcal{I}_{-1} + \mathcal{I}_0 + 1.$$

$$
\begin{aligned}
2q+2-N_1(E) &= 2\mathcal{I}_{-1}+2\mathcal{I}_0+2\mathcal{I}_1+2-N_1(E)\\
&= (2\mathcal{I}_{-1}+2\mathcal{I}_0+2\mathcal{I}_1+2)-(2\mathcal{I}_1+\mathcal{I}_0+1)\\
&= 2\mathcal{I}_{-1}+\mathcal{I}_0+1
\end{aligned}
$$

which we note is now a positive sum, rather than an alternating one, and in fact this sum is exactly $N_1(E^t)$.

Thus

$$N_2 = |E(\mathbb{F}_{q^2})| = |E(\mathbb{F}_q)| \cdot |E^t(\mathbb{F}_q)|.$$

This can also be proven via considering the trace of the Frobenius.

Question 3 *Is there a direct bijective proof of this identity?*

$$\begin{aligned} 2q + 2 - N_1(E) &= 2\mathcal{I}_{-1} + 2\mathcal{I}_0 + 2\mathcal{I}_1 + 2 - N_1(E) \\ &= (2\mathcal{I}_{-1} + 2\mathcal{I}_0 + 2\mathcal{I}_1 + 2) - (2\mathcal{I}_1 + \mathcal{I}_0 + 1) \\ &= 2\mathcal{I}_{-1} + \mathcal{I}_0 + 1 \end{aligned}$$

which we note is now a positive sum, rather than an alternating one, and in fact this sum is exactly $N_1(E^t)$.

Thus

$$N_2 = |E(\mathbb{F}_{q^2})| = |E(\mathbb{F}_q)| \cdot |E^t(\mathbb{F}_q)|.$$

This can also be proven via considering the trace of the Frobenius.

Question 3 *Is there a direct bijective proof of this identity?*

YES

Theorem 6 (M- 2005) *We have an explicit bijection θ in all cases between $E(\mathbb{F}_q) \times E'(\mathbb{F}_q)$ and $E(\mathbb{F}_{q^2})$. In some cases, it is additionally an isomorphism of groups.*

For example, when $I_0 = 0$ this bijection is an isomorphism. In this case, the bijection is given by

$$(P, Q) \mapsto P \oplus Q \text{ in } E(\mathbb{F}_{q^2}).$$

If $\mathcal{I}_0 = 1$, the addition map is a 2-to-1 map

If $\mathcal{I}_0 = 3$, the addition map is a 4-to-1 map

In these last two cases, explicit bijection θ is not just the addition map, but can be constructed by coset decomposition.

When $\mathcal{I}_0 = 0$, map θ is group theoretic as given above.

When $\mathcal{I}_0 = 3$, map θ is NEVER group theoretic.

When $\mathcal{I}_0 = 1$, we can choose the coset representatives to make θ an isomorphism depending on whether or not

$$\mathrm{ord}_2(|E(\mathbb{F}_q)|) \quad = \quad \mathrm{ord}_2(|E'(\mathbb{F}_q)|).$$

$$\textbf{Note}: \qquad \mathrm{ord}_2(n) \quad = \quad k \text{ if } n = 2^k m \text{ where } m \text{ is odd.}$$

III. A GEOMETRIC INTERPRETATION OF N_k.

$$N_k = \sum_{i=1}^{k} (-1)^{i-1} P_{k,i}(q) N_1^i$$

True in general: $N_1 \Big| N_k$ so want to understand second factor of $N_k = N_1 \cdot \tilde{N}_k$.

In fact, we can define sets $E^{(k)}(\mathbb{F}_q)$ for all k so that

$$|E^{(k)}(\mathbb{F}_q)| = \frac{N_k}{N_1}.$$

Let $E^{(k)}(\mathbb{F}_q)$ be the kernel of the Trace Map

$$\begin{array}{rcl} \Phi_k : E(\overline{\mathbb{F}_q}) & \rightarrow & E(\overline{\mathbb{F}_q}) \\ P & \mapsto & P \oplus \pi(P) \oplus \pi^2(P) \oplus \cdots \oplus \pi^{k-1}(P). \end{array}$$

In other words, $E^{(k)}(\mathbb{F}_q)$ equals the subset of points P in $E(\overline{\mathbb{F}_q})$ such that $\Phi_k(P) = P_\infty$.

$$\text{If } P \oplus \pi(P) \oplus \pi^2(P) \oplus \cdots \oplus \pi^{k-1}(P) = P_\infty$$

$$\text{Then } \pi(P) \oplus \pi^2(P) \oplus \pi^3(P) \oplus \cdots \oplus \pi^k(P) = \pi(P_\infty) = P_\infty$$

$$\text{Hence} \quad \pi^k(P) = P \qquad \text{and thus} \quad E^{(k)}(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k})$$

$$\text{Also } \pi(\Phi_k(P)) = \Phi_k(P) \quad \text{and thus} \quad \mathrm{Im}\ \Phi_k \subseteq E(\mathbb{F}_q)$$

We now wish to prove $E^{(k)}(\mathbb{F}_q) = \text{Ker } \Phi_k$ really satisfies

$$|E^{(k)}(\mathbb{F}_q)| = \frac{N_k}{N_1}.$$

We consider the chain complex

$$0 \longrightarrow E^{(k)}(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{\Phi_k} E(\mathbb{F}_q) \longrightarrow 0$$

which we prove is a short exact sequence.

We now wish to prove $E^{(k)}(\mathbb{F}_q) = \text{Ker } \Phi_k$ really satisfies

$$|E^{(k)}(\mathbb{F}_q)| = \frac{N_k}{N_1}.$$

We consider the chain complex

$$0 \longrightarrow E^{(k)}(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{\Phi_k} E(\mathbb{F}_q) \longrightarrow 0$$

which we prove is a short exact sequence.

Recall for $P \in E^{(k)}(\mathbb{F}_q)$,

$$\begin{aligned} \pi^k(P) = P &\quad \text{and thus} \quad E^{(k)}(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k}) \\ \pi(\Phi_k(P)) = \Phi_k(P) &\quad \text{and thus} \quad \text{Im } \Phi_k \subseteq E(\mathbb{F}_q) \end{aligned}$$

We now wish to prove $E^{(k)}(\mathbb{F}_q) = \text{Ker } \Phi_k$ really satisfies

$$|E^{(k)}(\mathbb{F}_q)| = \frac{N_k}{N_1}.$$

We consider the chain complex

$$0 \longrightarrow E^{(k)}(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \overset{\Phi_k}{\longrightarrow} E(\mathbb{F}_q) \longrightarrow 0$$

which we prove is a short exact sequence.

Recall for $P \in E^{(k)}(\mathbb{F}_q)$,

$$\begin{array}{lll} \pi^k(P) = P & \text{and thus} & E^{(k)}(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k}) \\ \pi(\Phi_k(P)) = \Phi_k(P) & \text{and thus} & \text{Im } \Phi_k \subseteq E(\mathbb{F}_q) \end{array}$$

Exactness if and only if

$$\text{Im } \Phi_k = E(\mathbb{F}_q).$$

One way to see this is to notice the following sequence is exact:

$$0 \longrightarrow E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{1-\pi} E^{(k)}(\mathbb{F}_q) \longrightarrow 0.$$

One way to see this is to notice the following sequence is exact:

$$0 \longrightarrow E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{1-\pi} E^{(k)}(\mathbb{F}_q) \longrightarrow 0.$$

Hilbert's Theorem 90 tells us that

$$Ker\ \Phi_k = E^{(k)}(\mathbb{F}_q) = Im\ (1-\pi)$$

and it is clear that $E(\mathbb{F}_q)$ is the kernel of $(1-\pi)$.

One way to see this is to notice the following sequence is exact:

$$0 \longrightarrow E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{1-\pi} E^{(k)}(\mathbb{F}_q) \longrightarrow 0.$$

Hilbert's Theorem 90 tells us that

$$Ker\ \Phi_k = E^{(k)}(\mathbb{F}_q) = Im\ (1-\pi)$$

and it is clear that $E(\mathbb{F}_q)$ is the kernel of $(1-\pi)$.

Furthermore,

$$Ker\ (1-\pi) = E(\mathbb{F}_q) = Im\ \Phi_k,$$

which implies the exactness of

$$0 \longrightarrow E^{(k)}(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_{q^k}) \xrightarrow{\Phi_k} E(\mathbb{F}_q) \longrightarrow 0.$$

Factoring N_k Completely:

Theorem 7 (M- 2005) *There exists polynomials, which we will denote as $ECyc_d$, in N_1 and q, only depending on d such that*

$$N_k(N_1, q) = \prod_{d|k} ECyc_d.$$

Moreover,

$$ECyc_d = \left| Ker\ Cyc_d(\pi) : E(\overline{\mathbb{F}_q}) \circlearrowleft \right|$$

where $Cyc_d(\pi)$ denotes the isogeny obtained from the dth Cyclotomic polynomial of the Frobenius map.

Example: Factoring N_6 Completely

$$N_6 = N_1\Big(2 + 2q - N_1\Big)\Big((3 + 3q + 3q^2) - (3 + 3q)N_1 + N_1^2\Big)\Big((1 - q + q^2) - (1 + q)N_1 + N_1^2\Big)$$

$$N_6 = E(\mathbb{F}_{q^6}) = Ker(1 - \pi^6)$$

$$N_2 = E(\mathbb{F}_{q^2}) = Ker(1 - \pi^2) \qquad N_3 = E(\mathbb{F}_{q^3}) = Ker(1 - \pi^3)$$

$$N_1 = E(\mathbb{F}_q) = Ker(1 - \pi)$$

$$Cyc_d(\pi) = \prod_{k|d}(1 - \pi^k)^{\mu(d/k)}$$

$$1 - \pi^6 = (1 - \pi)(1 + \pi)(1 + \pi + \pi^2)(1 - \pi + \pi^2)$$

$$
\begin{aligned}
ECyc_1 &= N_1 \\
ECyc_2 &= 2 + 2q - N_1 \\
ECyc_3 &= (3 + 3q + 3q^2) - (3 + 3q)N_1 + N_1^2 \\
ECyc_4 &= (2q^2 + 2) - (2q + 2)N_1 + N_1^2 \\
ECyc_5 &= (5 + 5q + 5q^2 + 5q^3 + 5q^4) - (10 + 15q + 15q^2 + 10q^3)N_1 \\
&+ (10 + 15q + 10q^2)N_1^2 - (5 + 5q)N_1^3 + N_1^4 \\
ECyc_6 &= (q^2 - q + 1) - (q + 1)N_1 + N_1^2
\end{aligned}
$$

Question 4 *Is there a combinatorial interpretation for these polynomials?*

Question 5 *How do these various combinatorial and geometric interpretations, including the original one of $|E(\mathbb{F}_{q^k})|$ all relate to each other?*