Honam Mathematical J. **19**(1997), No. 1,pp. 29–46

SUPERSINGULAR CURVES AND SPHERE PACKINGS

HWASIN PARK AND DAEYEOUL KIM

Dept. of Mathematics,
Chonbuk National University, Chonju 561-756, Korea.

1. Introduction

The sphere packing problem is to maximize the density and kissing number of balls in $\mathbb{R}^n$, not overlapping.

If $n \leq 3$, the answer is known so far. But, for $n \geq 4$, the problem is still open. To simplify this problem, we only consider the lattice packings. The lattice packing is the sphere packing centered at a lattice.

Now, an elliptic curve E is called *supersingular* if the endormorphism ring $\mathrm{End}(E)$ has rank 4.

If E, E' are elliptic curves, $L = \mathrm{Hom}(E', E)$ is an algebraic lattice (Lemma 4.1.)

In this paper, we prove the following.

If $K = \mathbb{C}$ and $j_E = 0$, then $\mathrm{End}(E) \cong A_2$, and if $K = \mathbb{F}_4$ and $j_E = 0$, then $\mathrm{End}(E) \cong D_4$ (Theorem 10.1.).

If J is an abelian variety of dimension g, then $\mathrm{Hom}(J, E)$ has rank $\leq 4g$ (Theorem 10.2.).

If E is supersingular over $\mathbb{F}_q$, with $q = p^f$, $p > 0$, the rank of $\mathrm{Hom}(J, E)$ is $\leq 4g$ (Theorem 10.4.).

2. $\mathrm{Hom}(F, E)$ and dual isogeny

Let F, E be elliptic curves over a field K. Then,

Received March 31, 1997.
This was partially supported by KOSEF, 1994, Grant No. 941-0100-014-2.

$$\begin{aligned}\mathrm{Hom}(F,E) &= \{\phi \in \mathrm{Mor}_K(F,E) : \phi(O_F) = O_E\} \\ &\cong \mathrm{Mor}_K(F,E)/\{\text{ translations}\} \\ &\cong \mathrm{Mor}_K(F,E)/\{\text{constant maps}\}\end{aligned}$$

is an abelian group.

Let F be defined by $g(u,v)=0$ and E be defined by $f(x,y)=0$.

Any isogeny $\phi : F \longrightarrow E$ is given by $\phi(u,v) = (x,y)$, where $x = R(u,v)$ and $y = S(u,v)$ are rational functions with $f(R,S) = 0$.

Therefore, $\mathrm{Mor}(F,E) \overset{\cong}{\longrightarrow} E(K(F))$ and this isomorphism gives $\{$ constant maps $\} \overset{\cong}{\longrightarrow} E(K)$.

Hence, $\mathrm{Hom}(F,E) \cong E(K(F))/E(K)$.

Now, let $\phi : F \longrightarrow E$ be an isogeny of degree m. Then there exists an isogeny $\widehat{\phi} : E \longrightarrow F$ of degree m such that $\widehat{\phi} \circ \phi = m$ and $\phi \circ \widehat{\phi} = m$.

We call it the *dual isogeny* of ϕ. Then, it has the following properties.

PROPOSITION 2.1.

(1) $\widehat{(\phi \circ \psi)} = \widehat{\psi} \circ \widehat{\phi}$
(2) $\widehat{(\phi + \psi)} = \widehat{\phi} + \widehat{\psi}$
(3) $\widehat{m} = m$
(4) $\hat{\hat{\phi}} = \phi$

3. Elliptic curves over $\mathbb{C}$

We consider the case that $K = \mathbb{C}$.

THEOREM 3.1. *Hom(F, E) is a free abelian group of rank* ≤ 2.

Proof. Let $E : y^2 = 4x^3 - g_2x - g_3$, where $\Delta \neq 0$.

Then, the invariant differential $w = \dfrac{dx}{y}$ is regular. And we have $E(\mathbb{C}) \overset{\cong}{\longrightarrow} \mathbb{C}/L$, via,

$P \mapsto \int_0^P \omega($ mod L), where $L = \{\int_\gamma \omega : \gamma \in H_1(E;\mathbb{Z})\}$.

Similarly, $F(\mathbb{C}) \cong \mathbb{C}/M$.

Let $\phi : F \longrightarrow E$ be an isogeny.

We have the following commutative diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\exists \alpha} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/M & \xrightarrow{\phi_\alpha} & \mathbb{C}/L \end{array}$$

The correspondence $\alpha \longleftrightarrow \phi_\alpha = \phi$ gives one-to-one correspondence.

Therefore, $\mathrm{Hom}(F, E) = \{\alpha \in \mathbb{C} : \alpha M \subset L\}$.

Here, $\deg \phi_\alpha = \sharp \ker \phi_\alpha = \sharp(\alpha^{-1}L/M) = \sharp(L/\alpha M)$.

Hence, $E \cong F$ if and only if $\exists \phi : F \longrightarrow E$ of degree 1 if and only if $\exists \alpha \neq 0$ such that $\alpha M = L$.

Put $M = \mathbb{Z}z_1 + \mathbb{Z}z_2$ and $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Any $\phi \in \mathrm{Hom}(F, E)$ is determined by α such that

$$\alpha z_1 = a\omega_1 + b\omega_2, \ \alpha z_2 = c\omega_1 + d\omega_2, \quad a, b, c, d \in \mathbb{Z}$$

But, α is completely determined by $\alpha z_1 = a\omega_1 + b\omega_2, \quad a, b \in \mathbb{Z}$.

Therefore, there is a map $\mathrm{Hom}(F, E) \longrightarrow \mathbb{Z}^2$ given by $\phi_\alpha \mapsto (a, b)$.

This map is injective, since ω_1, ω_2 are linearly independent.

Therefore, $\mathrm{Hom}(F, E) \hookrightarrow \mathbb{Z}^2$. This proves the theorem.

Let $R = \mathrm{End}(E) = \mathrm{Hom}(E, E) = \{\alpha \in \mathbb{C} : \alpha L \subset L\}$.

Then R contains $\mathbb{Z}$.

If $\mathrm{rank}(R) = 1$, then $R = \mathbb{Z}$.

Next we consider the case that $\mathrm{rank}(K) = 2$.

DEFINITION. Let K be a finitely generated $\mathbb{Q}$-algebra. Then *an order* R of K is a subring of K such that

(1) R is a finitely generated $\mathbb{Z}$-module, and
(2) $K = R \otimes \mathbb{Q}$.

EXAMPLE. Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field where $D < 0$, O_K the ring of integers in K, and $f \neq 0$ an integer. Then $R = \mathbb{Z} + fO_K$ is an order of K.

THEOREM 3.2. *If rank$(R) = 2$, R is an order of an imaginary quadratic field.*

Proof. Since $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \omega_1(\mathbb{Z} + \mathbb{Z}\tau)$ with $\tau = \dfrac{\omega_2}{\omega_1}$, we may assume $L = \mathbb{Z} + \mathbb{Z}\tau$.

Then, $\alpha = m + n\tau \quad (n \neq 0)$ and $\alpha\tau = m' + n'\tau$ for some $m, m', n, n' \in \mathbb{Z}$.

Therefore $a\tau^2 + b\tau + c = 0$.

Let $D = b^2 - 4ac$. Then $D < 0$, since $\tau \in \mathbb{C} - \mathbb{R}$ is a root of $a\tau^2 + b\tau + c = 0$.

Hence, $\alpha = m + n\tau \in \mathbb{Q}(\sqrt{D})$.

Actually, $R = \mathbb{Z} + \mathbb{Z}\dfrac{D + \sqrt{D}}{2}$.

THEOREM 3.3. *The set $\{F/\mathbb{C} : End(F) = R_D\}/\cong$ is finite, of order $\mathfrak{h}(R_D) = \sharp Pic(R_D)$.*

REMARK. $\mathfrak{h}(R_D) \approx |D|^{\frac{1}{2}}$

Proof.

$\mathrm{End}(F) \cong R$ if and only if lattice $M(\subseteq K)$ has endomorphisms exactly by R
if and only if M is a proper R-submodule of K of rank 2
if and only if M ia a projective R-module of rank 1.

Therefore,

$F \cong E$ if and only if $M = \alpha L$ for some $\alpha \in K^*$
if and only if the projective R-modules M, L are isomorphic

Hence, there exists a map $\{F : \mathrm{End}(F) = R\} \hookrightarrow \mathrm{Pic}(R)$, via, $F \mapsto$ the class of the lattice M of F.

For $M \in \mathrm{Pic}(R)$, if we put $F = \mathbb{C}/M$, $F \mapsto$ the class of the lattice M of F. Hence, this map is also surjective.

4. General Case

LEMMA 4.1. *Hom(F, E) is torsion-free.*

Proof. Let $\phi \neq 0$. If $m\phi = 0$, deg m deg $\phi = 0$
Since $\phi \neq 0$, deg $\phi \neq 0$.
Hence, deg $m = 0$. Therefore, $m = 0$.

LEMMA 4.2. *End(E) is an integral domain.*

Proof. Let $\phi \circ \psi = 0$. Then, deg ϕ deg $\psi = 0$
Therefore, deg $\phi = 0$ or deg $\psi = 0$, hence, $\phi = 0$ or $\psi = 0$.

THEOREM 4.1. *If l is prime to char(K), then* $E_l = \{P \in E(\overline{K}) : lP = 0\} \cong (\mathbb{Z}/l)^2$.

Proof. Let $K = \mathbb{C}$. Then, $E(\mathbb{C}) \cong \mathbb{C}/L$, and
$E_l \cong \frac{1}{l}L/L \cong L/lL \cong (\mathbb{Z}/l)^2$.

5. Tate Module

Let K be an arbitrary field and $l \in \mathbb{Z}$ be a prime with $l \neq$ char(K). Then, we get an inverse limit system

$$\cdots \longrightarrow E_{l^3} \xrightarrow{l} E_{l^2} \xrightarrow{l} E_l \xrightarrow{l} 0.$$

The (l-adic) *Tate module of E* is the group

$$T_l(E) = \lim_{\substack{\longleftarrow \\ n}} E_{l^n} \cong \mathbb{Z}_l \otimes \mathbb{Z}_l.$$

Let $\phi : F \longrightarrow E$ be an isogeny. Then $\phi \circ m_F = m_E \circ \phi$.
Take $m = l^n$, then we get the following commutative diagram

$$\begin{array}{ccc} F_{l^{n+1}} & \xrightarrow{\phi} & E_{l^{n+1}} \\ \downarrow & & \downarrow \\ F_{l^n} & \xleftarrow{\phi} & E_{l^n} \end{array}$$

This induces the map $\phi_l : T_lF \longrightarrow T_lE$ which is $\mathbb{Z}_l$-linear.

THEOREM(WEIL). *The natural map*

$$Hom_K(F,E)\otimes_{\mathbb{Z}}\mathbb{Z}_l \longrightarrow Hom_{\mathbb{Z}_l}(T_l(F),T_l(E))$$

given by $\phi \mapsto \phi_l$ *is injective.*

This is also surjective if

(1) *([9])* K *is a finite field;*
(2) *([3])* K *is a number field.*

COROLLARY. *Let* E *be an elliptic curve. Then End*(E) *is a free* $\mathbb{Z}$*-module of rank* $1,2,4$ *over* $\mathbb{Z}$.

Proof. $\mathrm{End}(E)\otimes\mathbb{Z}_l \hookrightarrow \mathrm{End}_{\mathbb{Z}_l}(T_l(F)) \cong \mathrm{End}_{\mathbb{Z}_l}(\mathbb{Z}_l\oplus\mathbb{Z}_l)$
Since any submodule of $\mathrm{End}_{\mathbb{Z}_l}(\mathbb{Z}_l\oplus\mathbb{Z}_l)$ has rank $1,2$ or 4, the corollary holds.

6. Quaternion algebra

DEFINITION. *A quaternion algebra* is an algebra of the form

$$A = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with the multiplication rules

$$\alpha^2,\beta^2 \in \mathbb{Q},\quad \alpha^2<0,\quad \beta^2<0,\quad \alpha\beta=-\beta\alpha.$$

The endomorphism ring of an elliptic curve is either $\mathbb{Z}$, an order in a quadratic imaginary field or an order in a quaternion algebra.

The last case occurs only when $p>0$.

EXAMPLE. Let $p=2, E: y^2+y=x^3$. Then, $\mathrm{End}(E)\cong \mathbb{Z}i+\mathbb{Z}j+\mathbb{Z}k+\mathbb{Z}\dfrac{-1+i+j+k}{2}$ where $i^2=j^2=-1, k=ij=-ji$, which is the Hamiltonian quaternion.

In this case, $\mathrm{End}(E)$ is called the Hurwitz order.

EXAMPLE. When $p=3$, and $E: y^2=x^3-x$ or when and $p=5$ and $E: y^2=x^3-1$ $\mathrm{End}(E)$ rank 4.

7. Supersingular curves

DEFINITION. An elliptic curve E over K is *supersingular* if $\mathrm{End}(E)$ has rank 4.

THEOREM 7.1. *We have the following.*

(1) *The map $p : E \longrightarrow E$ is purely inseperable, and $j(E) \in \mathbb{F}_{p^2}$.*
(2) *E is a supersingular curve if and only if $E(\overline{K})_p = 0$.*
(3) *E is a supersingular curve if and only if the invariant differential ω is exact, i.e., $\omega = dg$ for some rational function g.*

DEFINITION. Let $f(x,y) = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$ Then the *invariant differential* ω is defined as $\omega = \dfrac{dx}{f_y} = -\dfrac{dy}{f_x}$.

EXAMPLE. When $p = 2$ and $E : y^2 + y = x^3$, $\omega = \dfrac{dx}{2y+1} = dx$ is exact.

When $p = 3$ and $E : y^2 = x^3 - x$, $\omega = \dfrac{dy}{3x^2-1} = -dy$ is exact.

When $p = 5$ and $E : y^2 = x^3 - 1$, $\omega = \dfrac{dx}{2y} = \dfrac{dy}{3x^2} = \dfrac{dy}{-2x^2}$. Therefore $dx = 2y\omega$ and $dy = -2x^2\omega$.

Hence, $d(xy) = ydx + xdy = 2(y^2 - x^3)\omega = 2(-1)\omega = 3\omega$.

Hence, $\omega = d\left(\dfrac{xy}{3}\right)$, which is exact.

If $p = 2$, there exists a unique supersingular curve $y^2 + y = x^3$.

THEOREM 7.2. *Let K be a finite field of characteristic $p > 2$.*

(1) *Let E/K be an elliptic curve with Weierstrass equation*

$$E : y^2 = f(x),$$

where $f(x) \in K[x]$ is a cubic polynomial with distict roots (in $\overline{K}$). Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

(2) *Let* $m = \frac{p-1}{2}$ *and define a polynomial*

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$

Let $\lambda \in \overline{K}, \lambda \neq 0, 1$. *Then the elliptic curve*

$$E : y^2 = x(x-1)(x-\lambda)$$

is supersingular if and only if $H_p(\lambda) = 0$.

(3) *The polynomial* $H_p(t)$ *has distinct roots in* $\overline{K}$. *Up to isomorphism, there are exactly*

$$[p/12] + \epsilon_p$$

supersingular elliptic curves in characteristic p, *where* $\epsilon_3 = 1$, *and for* $p \geq 5$

$$\epsilon_p = 0, 1, 1, 2 \quad \textit{if} \quad p \equiv 1, 5, , 7, 11 (\textit{ mod } 12).$$

THEOREM 7.3. *If* $p = 11$, $E : y^2 = x(x-1)(x-\lambda)$ *is supersingular if and only if* $j = 0$ *or* 1.

Proof. $H_p(t) = t^5 + 3t^4 + t^3 + t^2 + 3t + 1 = (t^2 - t + 1)(t + 1)(t - 2)(t + 5)$ (mod11).

Therefore, E is supersingular if and only if $\lambda = -1, 2, -5$ or $\lambda^2 - \lambda + 1 = 0$ if and only if $j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = 0$ or $1 (= 1728)$.

THEOREM 7.4. *Let* $p \geq 5, E : y^2 = x^3 + 1$. *Then,* E *is supersingular if and only if* $p \equiv 2$ *(mod 3).* E *is non-supersingular if and only if* $p \equiv 1$ *(mod 3).*

Proof. We must compute the coefficient of x^{p-1} in $(x^3 + 1)^m$ where $m = \frac{p-1}{2}$.

$$(x^3+1)^m = \sum_{k=0}^{m} \binom{m}{k} x^{3k}.$$

If $p \equiv 2 \pmod 3$, then there exists no such k.
Hence, $(x^3+1)^m$ has no term of x^{p-1}.
Therefore, E is supersingular.
If $p \equiv 1 \pmod 3$, then the coefficient of x^{p-1} is $\binom{m}{k} = m(m-1)\cdots(m-k+1) \neq 0$ in $\overline{\mathbb{F}}_p$. Here, $k = \dfrac{p-1}{3}$.
Therefore, E is non-supersingular.

THEOREM 7.5. *Let $p \geq 3$, $E : y^2 = x^3 + x$, $j = 1728$. Then E is supersingular if and only if $p \equiv 3(\bmod 4)$, E is non-supersingular if and only if $p \equiv 1(\bmod 4)$.*

THEOREM (DEURING). *Let char$(K) = p$. Then*

$$\sum_{E:\text{supersingular}} \frac{1}{\sharp Aut(E)} = \frac{p-1}{24}.$$

Proof. Let $p = 2$, then there exists unique supersingular curve $y^2 + y = x^3$. Also, there exists 24 automorphisms on E if $j = 0$.
Let $p \neq 2$ and let $E; y^2 = x(x-1)(x-\lambda)$. Now, the Deuring polynomial $H_p(t)$ has distinct m roots. Also, j is a supersingular j-invariant if and only if $H_p(\lambda) = 0$.
Hence, there exists $\dfrac{p-1}{2}$ supersingular over K.
Now, $j(\lambda) = 2^8 \dfrac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.
This map has degree 6 with ramification at $\infty, 0, 12^3$.
The reason is following;
If $\lambda \neq \infty$, then $j = \infty$, and
$j'(\lambda) = 0$ if and only if λ is ramification, and hence
$3(\lambda^2-\lambda+1)^2(2\lambda-1)\lambda^2(\lambda-1)^2 = (\lambda^2-\lambda+1)^3 2\lambda(\lambda-1)(2\lambda-1)$, i.e.,
$\lambda = 0, \lambda - 1 = 0, \lambda = \dfrac{1}{2}, \lambda^2 - \lambda + 1 = 0$ or $3\lambda(\lambda-1) = 2(\lambda^2-\lambda+1)$, i.e.,

$\lambda = 0, \pm 1, 2, \frac{1}{2}$ or $\lambda^2 - \lambda + 1 = 0$.

If $\lambda^2 - \lambda + 1 = 0$, then $j = 0$.

If $\lambda = 0, 1$, then $j = \infty$.

If $\lambda = -1, 2, \frac{1}{2}$, then $j = 1728$.

If $j(\lambda) = j$ is supersingular with $j \neq \infty, 0, 1728$, then there exists 6 λ's with $j(\lambda) = j$.

If $j = 0$, then 2 λ's and if $j = \infty$ or 1728 then 3 λ's ($j \neq \infty$, since $\lambda \neq 0, 1, \infty$).

Now,

$$\frac{p-1}{2} = \sum_{\lambda:\text{supersingular}} 1 = 6 \sum_{\substack{E_\lambda:\text{supersingular} \\ j \neq 0,1728}} 1 + 3\alpha + 2\beta.$$

Here,

$$\alpha = \begin{cases} 0 & \text{if } j = 1728 \quad \text{(ordinary)}, \\ 1 & \text{if } j = 1728 \quad \text{(supersingular)}. \end{cases}$$

$$\beta = \begin{cases} 0 & \text{if } j = 0 \quad \text{(ordinary)}, \\ 1 & \text{if } j = 0 \quad \text{(supersingular)}. \end{cases}$$

Therefore,

$$\frac{p-1}{24} = \sum_{\substack{E_\lambda:\text{supersingular} \\ j \neq 0,1728}} \frac{1}{2} + \frac{\alpha}{4} + \frac{\beta}{6}.$$

If $j \neq 0, 1728$, $\text{Aut}(E) = \{\pm 1\}$. Therefore, $\mid \text{Aut}(E) \mid = 2$.

If $j = 0, \mid \text{Aut}(E) \mid = 6$.

If $j = 1728, \mid \text{Aut}(E) \mid = 4$.

Here, $$\frac{p-1}{24} = \sum_{E:\text{supersingular}} \frac{1}{|\text{Aut}(E)|}.$$

REMARKS.

(1) Let $E/\mathbb{Q}$. Then there exist infinitely many prime p such that $E/\mathbb{F}_p$ is ordinary.
(2) Let $E/\mathbb{Q}$. Then there exists infinitly many prime p such that $E/\mathbb{F}_p$ is supersingular.([2])
(3) Let E be CM. Then, the density of supersingular primes is 0, i.e.,

$$\lim_{x\to 0} \sharp\{p < x : \text{ supersingular prime }\}/\sharp\{p < x : p : \text{ is prime }\} = 0.$$

(4) **Conjecture** (Lang-Trotter[8])

$$\sharp\{p < x : p \text{ is a supersingular prime }\} \sim c\sqrt{x}/\log x \text{ as } x \to \infty.$$

8. Sphere packings and kissing numbers

Pack $\mathbb{R}^n$ with balls of equal radius $r > 0$, not overlapping. Then, we define *the density*

$$\rho = \lim_{\substack{D:\text{ box} \\ \mathrm{vol}(D)\to\infty}} \frac{\mathrm{vol}(P \cap D)}{\mathrm{vol}(D)} \leq 1,$$

and define *the kissing number*

$$\tau = \text{ the number of balls touching a fixed ball.}$$

PROBLEM. *Maximize ρ and τ for a given n.*

The best packing is the packing that ρ is the maximum.

EXAMPLE. If $n = 1$, then $\rho = 1,\ \tau = 2$.

EXAMPLE. If $n = 2$,

(1) square lattice packing($\mathbb{Z}_2$-lattice packing) : $\rho = \dfrac{\pi}{4}, \tau = 4$ (not best).

(2) hexagonal lattice packing(A_2-lattice packing) : $\rho = \dfrac{\pi}{2\sqrt{3}}, \tau = 6$ (best packing)

EXAMPLE. If $n = 3$, the face centered cubic lattice packing(A_3-packing) has $\rho = \dfrac{\pi}{\sqrt{18}}, \tau = 12$. This is the best packing proved by Hsiang(1990).

When $n = 3$, in 1694, I. Newton believed $\tau = 12$.
In 1694, D. Gregory beleived $\tau = 13$.
In 1874, Bender, Hoppe and in 1875, Günther proved $\tau = 12$.

9. Lattice packings

Let $v_1, v_2, \cdots, v_n$ be linearly independent vectors in $\mathbb{R}^N$. (Here, we assume $N \geq n$, and usually $N = n$). Let $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ be a lattice.

The *lattice packing* is the sphere packing centered at L.

EXAMPLE. Let $\mathbb{Z}_n = \mathbb{Z}^n$ be the n-dimensional cubic (or integer) lattice. Then $\tau = 2n$.

Take $r = \dfrac{1}{2}$, then

$$\rho_n = \text{ vol } B_n(\frac{1}{2}) = v_n(\frac{1}{2}) = \frac{v_n}{2^n},$$

where $B_n(r) = \{x \in \mathbb{R}^n \mid \|x\| < r\}, v_n(r) = \text{ vol } B_n(r)$ and $v_n = v_n(1)$.

LEMMA. $v_n = \dfrac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$

Proof. For any $n, r, v_n(r) = r^n v_n$.
Consider the unit n-ball

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2 = 1.$$

If $r = \sqrt{1 - x_n^2}$, then

$$\begin{aligned}
v_n &= \int_{-1}^{1} v_{n-1}(r)dx_n \\
&= 2\int_0^1 r^{n-1} v_{n-1}(r)dx_n \\
&= 2v_{n-1}\int_0^1 (\sqrt{1-x_n^2})^{n-1}dx_n \\
&= 2v_{n-1}\int_0^1 (\sqrt{1-t})^{\frac{n-1}{2}}\frac{dt}{2\sqrt{t}} \quad (\text{ where } t = x_n^2) \\
&= v_{n-1}\beta\left(\frac{n+1}{2},\frac{1}{2}\right) \\
&= v_{n-1}\frac{\Gamma(\frac{n+1}{2})\Gamma(\frac{1}{2})}{\Gamma(\frac{n+2}{2})}.
\end{aligned}$$

Now, $v_1 = 2$, hence,

$$\begin{aligned}
v_n &= \frac{\Gamma(\frac{n+1}{2})\Gamma(\frac{1}{2})}{\Gamma(\frac{n+2}{2})}\frac{\Gamma(\frac{n}{2})\Gamma(\frac{1}{2})}{\Gamma(\frac{n+1}{2})}\cdots\frac{\Gamma(\frac{3}{2})\Gamma(\frac{1}{2})}{\Gamma(\frac{5}{2})}v_1 \\
&= \frac{\Gamma(\frac{1}{2})^{n-1}\Gamma(\frac{3}{2})}{\Gamma(\frac{n+1}{2})}\cdot 2 \\
&= \frac{\Gamma(\frac{1}{2})^{n-1}\frac{1}{2}\Gamma(\frac{1}{2})}{\Gamma(\frac{n+1}{2})}\cdot 2 \\
&= \frac{\Gamma(\frac{1}{2})^{n}}{\Gamma(\frac{n}{2}+1)} = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}.
\end{aligned}$$

This proves the theorem.

Let $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ be a lattice in $\mathbb{R}^n$ and let

$$r = \frac{1}{2}\|l\|_{\min} = \frac{1}{2}\sqrt{< l, l >_{\min}}.$$

Then,

$$\rho = \lim_{\mathrm{vol}(D)\to\infty} \frac{v_n(r)\sharp(L\cap D)}{\mathrm{vol}(D)}.$$

$$\begin{aligned}\text{The volume of fundamental domain} &= \mathrm{vol}(\mathbb{R}^n/L)\\ &= \frac{\mathrm{vol}(D)}{\sharp(L\cap D)}\\ &= |\det(v_1, v_2, \cdots, v_n)|\end{aligned}$$

Therefore,

$$\begin{aligned}\rho &= \lim_{\mathrm{vol}(D)\to\infty} r^n v_n \frac{1}{|\det(v_1, v_2, \cdots, v_n)|}\\ &= \frac{v_n}{2^n}(\sqrt{< l, l >_{\min}})^n \frac{1}{|\det(v_1, v_2, \cdots, v_n)|}\\ &= \rho_n \mu(L)^{n/2},\end{aligned}$$

where $\mu(L) = \dfrac{< l, l >_{\min}}{\sqrt[n]{\det(L)}}$ and $\det(L) = \det(< v_i, v_j >) = \det(v_1, \cdots, v_n)^2$.

PROBLEM. *Maximize $\mu(L)$ over all lattice in $\mathbb{R}^n$. This is the best lattice packing*

EXAMPLE (A_2-LATTICE).
$\mu(L) = \dfrac{1}{|L|} = \dfrac{2}{\sqrt{3}}$, where $L = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$.
Hence, $\rho = \rho_2\mu(L)^{2/2} = \dfrac{\pi}{4}\dfrac{2}{\sqrt{3}} = \dfrac{\pi}{2\sqrt{3}}$.

EXAMPLE (A_3-LATTICE).

$$\mu(L) = |L|^{-2/3} = (\sqrt{2})^{2/3}, \text{ where } L = \begin{bmatrix} 1 & 0 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{6} & \sqrt{\frac{2}{3}} \end{bmatrix}.$$

$$\rho = \rho_3 \mu(L)^{3/2} = \frac{\frac{4}{3}\pi}{2^3}\sqrt{2} = \frac{\pi}{\sqrt{18}}.$$

Now, $\mathbb{R}^* O_n(\mathbb{R}) \setminus GL_n(\mathbb{R})/GL_n(\mathbb{Z}) \xrightarrow{\mu} \mathbb{R}$ is the space of all lattices in $\mathbb{R}^n$ up to orthogonal (conformal) equivalence, where $\mu(\alpha L) = \mu(L)$ for all $\alpha \in \mathbb{R}^*$.

EXAMPLE. If $n = 2$, then

$\mathbb{R}^* SO_2 = \mathbb{C}^* \setminus GL_2(\mathbb{R})/GL_2(\mathbb{Z})$ and $\mu = \dfrac{1}{\mathrm{Im}\tau}$.

Hence, $\mu_{\max} = \dfrac{2}{\sqrt{3}}$ and $\rho = \rho_2 \mu(L)^{2/2} = \dfrac{\pi}{\sqrt{12}}$.

Best lattice packings for $n \leq 8$.

$$\begin{pmatrix} n = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \text{Lattice} = & \mathbb{Z} & A_2 & A_3 & D_4 & D_5 & E_6 & E_7 & E_8 \\ \det L = & 2 & 3 & 4 & 4 & 4 & 3 & 2 & 1 \end{pmatrix},$$

when $n = 1, 2, 3$, they are the best sphere packing.

Here, $A_n = \{(x_0, x_1, \cdots, x_n) \in \mathbb{Z}^{n+1} \mid x_0 + \cdots + x_n = 0\}$

$D_n = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \text{ is even}\}$. If $n = 3$, $A_3 \approx D_3$.

For $n \equiv 0 (\mathrm{mod}\ 8)$,

$$E_n = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n \mid \sum x_i \equiv 0 \pmod 2)\} + \mathbb{Z}\left(\frac{1}{2}, \cdots, \frac{1}{2}\right)$$

$$= \{(x_1 + \frac{1}{2}, \cdots, x_n + \frac{1}{2}) \mid x_i \in \mathbb{Z}, \sum x_i \equiv 0 \pmod 2).\}$$

$E_7 = \{x \in E_8 : x_7 = x_8\}$

$E_6 = \{x \in E_8 : x_6 = x_7 = x_8\}$

For $8 < n \leq 24$, the Leech lattice Λ_{24} and its slices are conjectured "best".

10. Algebraic lattices

An algebraic lattice is a free $\mathbb{Z}$-module L of rank n with $Q : L \longrightarrow \mathbb{Z}$ positive-definite quadratic form $Q : L \longrightarrow \mathbb{Z}$.

THEOREM 10.1. Let E, E' be elliptic curves over K and L =Hom(E', E).

If $K = \mathbb{C}$, $E' = E$ with $j_E = 0$, then, $L \cong A_2$-lattice.

If $K = \mathbb{F}_4$, $E' = E$ with $j_E = 0$, then, $L \cong D_4$-lattice.

Proof. If we let $Q(\phi) =$ deg ϕ, then Q is a positive-definite quadratic form. Hence we clearly get the result.

For example, if

$$E : y^2 = x^3 + 1, j = -1728\frac{(4a)^3}{\Delta} = 0,$$

then End$(E) \cong A_2$.

And, if $E : y^2 = x^3 + x$, then End$(E) \cong D_4$.

Now,

$$\begin{aligned} L &= \mathrm{Hom}(E', E) \\ &= \{\phi : E' \longrightarrow E \mid \phi(0') = 0\} \\ &= \mathrm{Mor}_k(E', E)/\{\text{translations}\}. \end{aligned}$$

Let E' be given by $g(u, v) = 0$, and let $\phi(u, v) = (x, y)$ with $x = R(u, v)$, $y = S(u, v)$ where R, S are rational functions in u, v such that $f(R, S) = 0$.

Hence, Mor$(E', E) \cong E(K(E'))$ and { constant maps } $\cong E(K)$.

Therefore, $L \cong E(K(E'))/E(K) \cong \mathrm{Mor}_K(E', E)/\{\text{constants}\}$.

Replace E' by a curve X of any genus g. Then, L is a free abelian group of rank $\leq 4g$ with $Q(\phi) = \deg\phi$.

Let J be an abelian variety of dim g (or, $J =$ Jacobian of E). Then, L =Hom(J, E) has rank $L=$ ($\sharp$ of occurences of E in J) rank(End(E)) $\leq 4g$.

For example, take $J = E^g$.

Consequently, we have the following theorem.

THEOREM 10.2. *Let J be an abelian variety of dimension g. Then $L = Hom(J, E)$ has rank $\leq 4g$.*

THEOREM 10.3. *Let $x^3y + y^3z + z^3x = 0$ be Klein quartic. If $K = \mathbb{C}$, L has rank 6.*
Then $J \cong E^3$ and $j = -3^3 \cdot 5^3$.
This is a curve with complex multiplication by $D = -7$.
If $K = \mathbb{C}$ then L has rank $= 6$, $detL = 7^3$ and $< l, l >_{\min} = 4$.

THEOREM 10.4. *In characteristic $p > 0$, $J = E^g$, E is supersingular over $\mathbb{F}_q$ with $q = p^f$. Then, rank of $Hom(J, E)$ is $4g$.*

Proof. $X : x^{q+1} + y^{q+1} + z^{q+1} = 0$ has a non-trivial automorphism, via $\alpha \mapsto \alpha^q = \overline{\alpha}$.
Take $g = \dfrac{q(q-1)}{2}$.
Then, $N(X/\mathbb{F}_{q^2}) = q^3 + 1$, and $G = PU_3(q)$ acts on X.
If $q \equiv 2(\bmod 3)$,

$$E : u^3 + v^3 + w^3 = 0 \text{ is supersingular in char } p.$$

There exists a map

$$x^{q+1} + y^{q+1} + z^{q+1} = 0 \longrightarrow u^3 + v^3 + w^3 = 0$$

where $u = x^{\frac{q+1}{3}}, v = y^{\frac{q+1}{3}}, \omega = z^{\frac{q+1}{3}}$.
Therfore, $\text{Hom}(J, E) \neq 0$ and rank is $2q(q-1) = 4g$.

COROLLARY. *Let $p = 2$ and $q = 2^2 = 4$.*
$X : x^5 + y^5 + z^5, E : y^2 = x^3 + x$. Then, $g = 6$,
$L = Hom(X, E)$ has rank 24.
Then, $L \cong \Lambda_{24}$.

References

1. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer- Verlag, 1988.
2. N. Elkies, *The existence of infinite many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (1987), 561–567.
3. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

4. Husemoller, D., *Symetric Bilinear Forms*, Springer-Verlag, New York, 1973.
5. ———, *Elliptic Curves*, Springer-Verlag, New York, 1987.
6. Lang, S., *Algebraic Number Theory*, Addison-Wesley, 1970.
7. ———, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
8. Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, New York, 1986.
9. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.