JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **22**, No. 3, September 2009

ISOMORPHISM CLASSES OF ELLIPTIC CURVES OVER FINITE FIELDS WITH CHARACTERISTIC 3

Eunkyung Jeong*

Abstract. We count the isomorphism classes of elliptic curves over finite fields $\mathbb{F}_{3^n}$ and list a representative of each isomorphism class. Also we give the number of rational points for each supersingular elliptic curve over $\mathbb{F}_{3^n}$.

1. Introduction

Elliptic curves have been intensively studied in algebraic geometry and number theory. Starting in about 1985, the theory of elliptic curves over finite fields has been applied to various problems; factoring integers, primality proving and construction of public key cryptosystems. One of the advantages using elliptic curve cryptosystems is the greater flexibility in choosing the group. That is for each prime power q there is only one multiplicative group $\mathbb{F}_q^*$, but there are many elliptic curve groups.

It may be useful to classify the isomorphism classes of elliptic curves over finite fields, in order to know how many essentially different choices of curves are. And this classification is used to produce nonisomorphic elliptic curves, which may be useful for a cryptographic purpose. In [4] isomorphism classes of elliptic curves over $\mathbb{F}_{p^n}, p \neq 2, 3$ and $\mathbb{F}_{2^n}$ were studied.

In this paper we count the isomorphism classes of elliptic curves defined over finite fields $\mathbb{F}_{3^n}$ and list a representative of each isomorphism class. Moreover, we give the order and the group structure of supersingular elliptic curves over $\mathbb{F}_{3^n}$. This fields are getting more interest in a cryptographic purpose (see, for instance, [1] and [2]).

Received April 14, 2009; Accepted August 14, 2009.
2000 Mathematics Subject Classification: Primary 11G05, 11G20, 11G30.
Key words and phrases: elliptic curves, finite field, isomorphism classes.
This work was supported by the Korea Research Foundation Grant funded by the Korea Government(MOEHRD, Basic Research Promotion Fund) (KRF-2005-075-C00005).

This paper is organized as follows;

In section 2 the necessary definitions and notations are introduced. In section 3 the exact number and a set of representatives of the isomorphism classes of elliptic curves over $\mathbb{F}_{3^n}$ are produced. In section 4 we give the number of points and the group type of supersingular elliptic curves over finite fields with characteristic 3.

2. Elliptic curves

In this section, we recall the basic definitions and properties about the elliptic curves. We follow notations given in [4].

If $\mathbb{K}$ is a field, let $\bar{\mathbb{K}}$ denote its algebraic closure. A *Weierstrass equation* is a homogeneous equation of degree 3 of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_i \in \mathbb{K}$. The Weierstrass equation is said to be smooth or non-singular if for all projective points $P(X, Y, Z) \in P^2(\bar{\mathbb{K}})$ satisfying

$$F(X, Y, Z) = Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3 = 0,$$

at least one of the three partial derivatives $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ is non-zero at P. An *elliptic curve* E is the set of all solutions in $P^2(\bar{\mathbb{K}})$ of a smooth Weierstrass equation. There is exactly one point in E with Z-coordinate equal to 0, namely $(0, 1, 0)$. We call this point the *point at infinity* and denote it by $\mathcal{O}$.

For convenience, we will write the Weierstrass equation for an elliptic curve using non-homogeneous (affine) coordinates $x = X/Z, y = Y/Z$,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

An elliptic curve E is then the set of solutions to equation (2.1) in the affine plane $A^2(\bar{\mathbb{K}}) = \bar{\mathbb{K}} \times \bar{\mathbb{K}}$, together with the extra point at infinity $\mathcal{O}$. If $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$, the E is said to be defined over $\mathbb{K}$, and we denote by $E/\mathbb{K}$. If E is defined over $\mathbb{K}$, then the set of $\mathbb{K}$-rational points of E, denoted $E(\mathbb{K})$, is the set of points both of whose coordinates lie in $\mathbb{K}$, together with the point $\mathcal{O}$.

The following lemma will be needed for theorems in the later sections.

Lemma 2.1. [3] *The trinomial*

$$x^p - x - a, \quad a \in \mathbb{F}_q,$$

where q is a prime power p^n, has a solution in F_q if and only if $Tr(a) = 0$. Here, $Tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$.

3. Isomorphism classes of elliptic curves over $\mathbb{F}_q, q = 3^n$

Let E be an elliptic curve over a field $\mathbb{K}$. We can write E as the following nonsingular Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$.

Two elliptic curves are said to be *isomorphic* if they are isomorphic as projective varieties. Briefly, two projective varieties V_1, V_2 defined over a field $\mathbb{K}$ are isomorphic over $\mathbb{K}$ if there exist morphisms $\phi : V_1 \longrightarrow V_2, \psi : V_2 \longrightarrow V_1(\phi, \psi$ defined over $\mathbb{K})$, such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on V_1, V_2 respectively. The following result relates the notion of isomorphism of elliptic curves to the coefficients of the Weierstrass equations that define the curves [4].

THEOREM 3.1. [4] *Two elliptic curves $E_1/\mathbb{K}$ and $E_2/\mathbb{K}$ given by the equations*

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$$E_2 : y^2 + \bar{a_1}xy + \bar{a_3}y = x^3 + \bar{a_2}x^2 + \bar{a_4}x + \bar{a_6}$$

are isomorphic over $\mathbb{K}$ if and only if there exists an admissible change of variables $u, r, s, t \in \mathbb{K}, u \neq 0$, such that the change of variables

$$(x, y) \rightarrow (u^2x + r, u^3y + u^2sx + t)$$

transforms equation E_1 to equation E_2. The relationship of isomorphism is an equivalence relation.

THEOREM 3.2. [4] *Two elliptic curves $E_1/\mathbb{K}$ and $E_2/\mathbb{K}$ are isomorphic over $\mathbb{K}$ if and only if there exist $u, r, s, t \in \mathbb{K}, u \neq 0$, that satisfy the following equations;*

$$\begin{cases} u\bar{a_1} = a_1 + 2s \\ u^2\bar{a_2} = a_2 - sa_1 + 3r - s^2 \\ u^3\bar{a_3} = a_3 + ra_1 + 2t \\ u^4\bar{a_4} = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6\bar{a_6} = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{cases}$$

PROPOSITION 3.3. [6] *Let $E/\mathbb{F}_q, q = 3^n$ be a curve given by a Weierstrass equation. Then there is an admissible change of variables*

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \text{ with } u \in \mathbb{F}_q^* \text{ and } r, s, t \in \mathbb{F}_q$$

such that $E/\mathbb{F}_q$ has a Weierstrass equation of the indicated form.

$$\begin{cases} y^2 = x^3 + a_2x^2 + a_6, & \Delta(E) = -a_2^3a_6,\ j(E) = -a_2^3/a_6 \ \text{ if } j(E) \neq 0, \\ y^2 = x^3 + a_4x + a_6, & \Delta(E) = -a_4^3 \text{ if } \ j(E) = 0, \end{cases}$$

where $\Delta(E)$ denotes the discriminant of E.

The elliptic curve E is said to be supersingular if p divides t, where $\sharp E(\mathbb{F}_q) = q+1-t, q = p^n$. Then it is well-known that E is supersingular if and only if j-invariant $j(E) = 0$ when $q = 3^n$.

THEOREM 3.4. *(Nonsupersingular case) There are $2(q-1)$ isomorphism classes of non-supersingular elliptic curves over $\mathbb{F}_q, q = 3^n$.*

Proof. Let E_1, E_2 be non-supersingular elliptic curves defined over $\mathbb{F}_{3^n}$ and given by the equations

$$E_1 : y^2 = x^3 + a_2x^2 + a_6, \quad (a_2 \neq 0, a_6 \neq 0),$$
$$E_2 : y^2 = x^3 + \bar{a_2}x^2 + \bar{a_6}, \quad (\bar{a_2} \neq 0, \bar{a_6} \neq 0).$$

Then the only admissible change of variables which transforms E_1 into E_2 is

$$(x, y) \to (u^2x, u^3y), u \in \mathbb{F}_q^*,$$

such that $u^2\bar{a_2} = a_2$ and $u^6\bar{a_6} = a_6$. When $u^2 = 1$, the above transformation gives the automorphism. So there are $(q-1)^2/((q-1)/2) = 2(q-1)$ isomorphism classes of non-supersingular elliptic curves over $\mathbb{F}_q, q = 3^n$. □

THEOREM 3.5. *(Supersingular case) There are 6 isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{3^n}$, when n is even. There are 4 isomorphism classes of supersingular elliptic curves, when n is odd.*

Proof. Let E be a supersingular elliptic curve over $\mathbb{F}_{3^n}$ given by the following equation.

$$E : y^2 = x^3 + a_4x + a_6, \ \ a_4 \neq 0.$$

The admissible change of variables in the equation E which transforms into itself is

$$(x, y) \to (u^2x + r, u^3y),$$

where

$$u^4 = 1 \text{ and } u^6a_6 = a_6 + a_4r + r^3.$$

Substitute $u^4 = 1$ into the second equation above, then we obtain

$$r^3 + a_4 r + a_6(1 - u^2) = 0. \tag{3.1}$$

We split this into the following cases;
If $\sqrt{-a_4} \notin \mathbb{F}_q^*$, then the map $r \mapsto r^3 + a_4 r$ is bijective. Hence the equation (3.1) has unique solution, say r_u, and the automorphism group is

$$(x, y) \to (u^2 x + r_u, u^3 y).$$

If $\sqrt{-a_4} \in \mathbb{F}_q^*$, then there exists $r_0 \in \mathbb{F}_q^*$ such that $r_0^2 = -a_4$, and the equation (3.1) has a solution in $\mathbb{F}_q$ iff the equation

$$r^3 - r = a_6(u^2 - 1)/r_0^3 \tag{3.2}$$

has a solution in $\mathbb{F}_q$. If $Tr(a_6(u^2-1)/r_0^3) \neq 0$, then the equation (3.2) has no solutions by Lemma 2.2. If $Tr(a_6(u^2 - 1)/r_0^3) = 0$, then the equation (3.2) has three solutions; If $\bar{r_u}$ is one of them, the other solutions are $\bar{r_u} \pm 1$. Note that since $u^2 = \pm 1 \in \mathbb{F}_3$, the condition $Tr(a_6(u^2-1)/r_0^3) = 0$ iff $u^2 Tr(a_6/r_0^3) - Tr(a_6/r_0^3) = 0$.

We further split this into two cases according to n is even or odd. When n is even, then the solutions of the equation $u^4 = 1$ are $\{\pm 1, \pm\zeta | \zeta^2 = -1, \zeta \in \mathbb{F}_q\}$. If $Tr(a_6/r_0^3) = 0$, then the automorphism group is

$$(x, y) \mapsto (u^2 x + r, u^3 y), u^4 = 1, r \in \{r_0 \bar{r_u}, r_0(\bar{r_u} \pm 1)\}.$$

If $Tr(a_6/r_0^3) \neq 0$, then the automorphism group is

$$(x, y) \mapsto (x + r, uy), u^2 = 1, r \in \{0, \pm r_0\}.$$

When n is odd, the solutions to the equation $u^4 = 1$ are $\{\pm 1\}$. So the automorphism group is

$$(x, y) \mapsto (x + r, uy), u^2 = 1, r \in \{0, r_0, -r_0\}.$$

In conclusion, if n is even, the number of supersingular elliptic curves is

$$\frac{q(q-1)/2}{q(q-1)/4} + \frac{q(q-1)/6}{q(q-1)/12} + \frac{q(q-1)/3}{q(q-1)/6} = 6,$$

and if n is odd, the number of supersingular elliptic curves is

$$\frac{q(q-1)/2}{q(q-1)/2} + \frac{q(q-1)/2}{q(q-1)/6} = 4.$$

□

THEOREM 3.6. *1.(Nonsupersingular case) A set of representatives of the isomorphism classes of non-supersingular elliptic curves over* $\mathbb{F}_{3^n}$ *is*

$$\{y^2 = x^3 + a_2 x^2 + a_6 | \ a_2 \in \{1, \alpha\}, a_6 \in \mathbb{F}_{3^n}^*\},$$

where α is a quadratic nonresidue in $\mathbb{F}_{3^n}^*$
2. (Supersingular case) A representative from each isomorphism class of supersingular elliptic curves over $\mathbb{F}_{3^n}$ is

$$\begin{cases} y^2 = x^3 - \beta x \\ y^2 = x^3 - \beta^3 x \\ y^2 = x^3 - x \\ y^2 = x^3 - \gamma x \\ y^2 = x^3 - x + \delta \\ y^2 = x^3 - \gamma x + \delta \end{cases} \quad \text{if } n \text{ is even,}$$

where $\sqrt{\beta} \notin \mathbb{F}_{3^n}^*$, $\sqrt{\gamma} \in \mathbb{F}_{3^n}^*$, $\sqrt[4]{\gamma} \notin \mathbb{F}_{3^n}^*$ and $Tr(\delta) \neq 0$.
And

$$\begin{cases} y^2 = x^3 + x \\ y^2 = x^3 - x \\ y^2 = x^3 - x + \lambda \\ y^2 = x^3 - x + \mu \end{cases} \quad \text{if } n \text{ is odd,}$$

where $Tr(\lambda) = 1, Tr(\mu) = -1$.

4. Number of points

We determine the number of rational points $\sharp E(\mathbb{F}_{3^n})$, where E is a supersingular curve over $\mathbb{F}_{3^n}$. We summarize the needed Theorems to count the order of supersingular elliptic curves and to find the group structure.

THEOREM 4.1. *(Weil Theorem) Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $t = q + 1 - \sharp E(\mathbb{F}_q)$. Then $\sharp E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \beta^k$, where α, β are complex numbers determined from the factorization of $1 - tT + qT^2 = (1 - \alpha T)(1 - \beta T)$.*

THEOREM 4.2. [7] *Let p be a prime and $q = p^m$. Let t be and integer with $|t| \leq 2\sqrt{q}$ and $N_q(t)$ be the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ such that $\sharp E(\mathbb{F}_q) = q + 1 - t$. Then*

$$N_q(t) = \begin{cases} H(t^2-4q), & \text{if } t^2 < 4q, \text{ and } p \nmid t \\ H(-4p), & \text{if } t = 0 \text{ and } m \text{ odd.} \\ 1, & \text{if } t^2 = 2q, \text{ and } p = 2, m \text{ odd.} \\ 1, & \text{if } t^2 = 3q, \text{ and } p = 3, m \text{ odd.} \\ \frac{1}{12}(p+6-4(\frac{-3}{p})-3(\frac{-4}{p})), & \text{if } t^2 = 4q, \text{ and } m \text{ even.} \\ 1-(\frac{-3}{p}), & \text{if } t^2 = q, \text{ and } m \text{ even.} \\ 1-(\frac{-4}{p}), & \text{if } t = 0, \text{ and } m \text{ even.} \\ 0, & \text{otherwise} \end{cases}$$

Here, $H(\Delta)$ denotes the Kronecker class number of Δ, and is the number of $SL_2(\mathbb{Z})$-orbits of positive definite binary quadratic forms of discriminant Δ, where Δ is a negative integer congruent to 0 or 1 modulo 4.

THEOREM 4.3. [5] *Let $\sharp E(\mathbb{F}_q) = q+1-t$.*

1. *If $t^2 = q, 2q$, or $3q$, then $E(\mathbb{F}_q)$ is cyclic.*
2. *If $t^2 = 4q$, then either $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ or $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$, depending on whether $t = 2\sqrt{q}$ or $t = -2\sqrt{q}$ respectively.*
3. *If $t = 0$ and $q \not\equiv 3 \pmod 4$, then $E(\mathbb{F}_q)$ is cyclic. If $t = 0$ and $q \equiv 3 \pmod 4$, then $E(\mathbb{F}_q)$ is cyclic or $E(\mathbb{F}_q) \cong \mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$.*

The curve E can be also viewed as an elliptic curve over any extension field $\mathbb{F}_{q^m}$. One can compute $\sharp E(\mathbb{F}_{q^m})$, for $m \geq 2$, from $\sharp E(\mathbb{F}_q)$ using the Weil theorem. The group type of these curves may be determined by using Theorem 4.3.

THEOREM 4.4. *The number of points and the group structure of supersingular elliptic curves in Theorem 3.6 are given following tables;*

No	*Curve E*	n	$\sharp E(\mathbb{F}_{3^n})$	*Group Type*
1	$y^2 = x^3 - \beta x$	*even*	$q+1$	*cyclic*
2	$y^2 = x^3 - \beta^3 x$	*even*	$q+1$	*cyclic*
3	$y^2 = x^3 - x$	$n \equiv 0 \pmod 4$	$q+1-2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$
		$n \equiv 2 \pmod 4$	$q+1+2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$
4	$y^2 = x^3 - \gamma x$	$n \equiv 0 \pmod 4$	$q+1+2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$
		$n \equiv 2 \pmod 4$	$q+1-2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$
5	$y^2 = x^3 - x + \delta$	*even*	$q+1 \pm \sqrt{q}$	*cyclic*
6	$y^2 = x^3 - \gamma x + \delta$	*even*	$q+1 \mp \sqrt{q}$	*cyclic*

Table 1. Orders of supersingular elliptic curves over $\mathbb{F}_{3^n}$, where n is even

No	*Curve E*	n	$\sharp E(\mathbb{F}_{3^n})$	*Group Type*
1	$y^2 = x^3 + x$	*odd*	$q+1$	*cyclic*
2	$y^2 = x^3 - x$	*odd*	$q+1$	$\mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$
3	$y^2 = x^3 - x + \lambda$	*odd*	$q+1 \pm \sqrt{3q}$	*cyclic*
4	$y^2 = x^3 - x + \mu$	*odd*	$q+1 \mp \sqrt{3q}$	*cyclic*

Table 2. Orders of supersingular elliptic curves over $\mathbb{F}_{3^n}$, where n is odd

Proof. When n be even, let $\sharp E_i = \sharp E_i(\mathbb{F}_q) = q + 1 - t_i$, for $1 \le i \le 6$, where $q = 3^n$ and the curves E_i are those of Theorem 3.6 (when n is even). We first observe that

$$\{x^3 - \beta x | x \in \mathbb{F}_q\} = \{x^3 - \beta^3 x | x \in \mathbb{F}_q\} = \mathbb{F}_q,$$

since β is a quadratic nonresidue in $\mathbb{F}_q$. Hence $t_1 = t_2 = 0$. Since the coefficients of the equation E_3 are in $\mathbb{F}_3$, we can apply the Weil Theorem to determine $\sharp E_3$ and we get $t_3 = 2\sqrt{q}$ or $-2\sqrt{q}$ according to whether $n \equiv 2$ or $0 \pmod 4$ respectively.
By Theorem 4.2, we obtain that the 6 values of t_i are $0, 0, \pm\sqrt{q}$ and $\pm\sqrt{2q}$ (not necessarily in that order). We find E_4 has four 2-torsion points since γ is a quadratic residue in $\mathbb{F}_q$. Hence $E_4(\mathbb{F}_q)$ cannot be cyclic, so $t_4 = \pm 2\sqrt{q}$.

Therefore $t_5 = \pm\sqrt{q}$ and $t_6 = -t_5$.

When n is odd, there are 4 isomorphism classes of supersingular curves over $\mathbb{F}_{3^n}$. Let $\sharp E_i = \sharp E_i(\mathbb{F}_q) = q + 1 - t_i$, for $1 \le i \le 4$, where $q = 3^n$ and the curves E_i are those of Theorem 3.6 (when n is odd). We determine the order of curves $E_i (= q + 1), i = 1, 2$ over $\mathbb{F}_{3^n}$ from $\sharp E(\mathbb{F}_3)(=4)$ using the Weil theorem.
Since there are two(four) 2-torsion points in the curve $E_1(E_2)$, the group structure is cyclic ($\mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$).
By Theorem 4.2, we obtain that the 4 values of t_i are $0, 0, \sqrt{3q}$ and $-\sqrt{3q}$ (not necessarily in that order). Since $t_1 = t_2 = 0$, we get $t_3 = \pm\sqrt{3q}$ and $t_4 = -t_3$. $\square$

If $n \not\equiv 0 \pmod 3$, then $Tr(1) \ne 0$ and $Tr(-1) \ne 0$. So we can take $\lambda = 1, \mu = -1$ or $\lambda = -1, \mu = 1$ depending on $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$ respectively in E_3, E_4 when n is odd. The order of the curve $y^2 = x^3 - x + 1$ is $q + 1 + \sqrt{3q}$ if $n \equiv \pm 1 \pmod{12}$ and $q + 1 - \sqrt{3q}$ if $n \equiv \pm 5 \pmod{12}$. The order of the curve $y^2 = x^3 - x - 1$ is $q + 1 - \sqrt{3q}$ if $n \equiv \pm 1 \pmod{12}$ and $q + 1 + \sqrt{3q}$ if $n \equiv \pm 5 \pmod{12}$.

References

[1] S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, *Efficient Algorithms for Pairing-Based Cryptosystems*, eprint 2002/008.

[2] D. Boneh, B. Lynn and H. Scham, *Short signatures from the Weil pairing*, Proc. of Asiacrypt'01, 514-532, 2001.

[3] R. Lidi and H. Niederreiter, *Finite fields, Encyclopedia of Math and its application*, **20**, Addison-Wesley, 1983.

[4] A. Menezes and N. Koblitz, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.

[5] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory A, **46** (1987), 183-211.

[6] J. Silverman, *The Arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[7] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. **2** (1969), 521-560.

*

Department of Mathematics
Konkuk University
Seoul 143-701, Republic of Korea
E-mail: ekjeong@konkuk.ac.kr