J. Korean Math. Soc. **47** (2010), No. 1, pp. 101–112
DOI 10.4134/JKMS.2010.47.1.101

IRREDUCIBILITY OF POLYNOMIALS AND DIOPHANTINE EQUATIONS

Sung Sik Woo

Abstract. In [3] we showed that a polynomial over a Noetherian ring is divisible by some other polynomial by looking at the matrix formed by the coefficients of the polynomials which we called the resultant matrix. In this paper, we consider the polynomials with coefficients in a field and divisibility of a polynomial by a polynomial with a certain degree is equivalent to the existence of common solution to a system of Diophantine equations. As an application we construct a family of irreducible quartics over $\mathbb{Q}$ which are not of Eisenstein type.

1. Introduction

In this paper we show that the reducibility of a polynomial is the same as the existence of the solutions to some Diophantine equations. To determine whether a Diophantine equation has a solution or not is not, of course, easier than to determine whether a polynomial is irreducible or not. However the problems of Diophantine equations has a long history and there are a large amount of results which are available to use. Therefore we expect to use those results to deduce the results on irreducibility of polynomials and *vice versa*.

In Section 2, we recall the resultant matrix of polynomials and a criterion for divisibility of polynomials by using the resultant matrix which is shown in [3]. Then we show that irreducibility of a polynomial over a Noetherian domain is equivalent to the existence of common solution of some Diophantine equations.

In Section 3, for a given polynomial, we give an explicit description of the Diophantine equations whose existence of a common solution is equivalent to the existence of a divisor of the polynomial.

In Section 4, using the result on the group structure of rational points on elliptic curves we construct a 'family' of irreducible quartics which are non-Eisensteinian. In Section 5, we make a few remarks on irreducibility of quintics.

Throughout all rings are commutative with the identity 1.

Received March 3, 2008.

2000 *Mathematics Subject Classification.* 11R09, 13B25, 14G05, 11G05.

Key words and phrases. irreducible polynomial, Diophantine equations, rational points of elliptic curves.

2. Resultant matrix and divisibility of polynomials

In this section we recall the result of [3] which we will use later. To fix our notations let A be a commutative ring and F_1, F_2 be A-free modules with bases $\beta = \{v_1, v_2, \dots, v_n\}$ and $\gamma = \{w_1, w_2, \dots, w_m\}$ of F_1 and F_2 respectively. Let $\phi : F_1 \to F_2$ be an A-linear map. Then the matrix $X = (x_{ij}) \in M(n \times m, A)$ of ϕ with respect to the bases β and γ is defined by the equality

$$\phi(v_i) = \sum_{j=1}^{m} x_{ij} w_j \ (i = 1, 2, \dots, n).$$

Here we denote the matrices of size $n \times m$ with coefficients in A by $M(n \times m, A)$. If $\psi : F_2 \to F_3$ is another A-linear map of free modules with matrix Y, then the matrix corresponding to $\psi \circ \phi$ will be XY. Let A be a commutative ring. For positive integers n, m let $f, g \in A[X]$ be the polynomials

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0,$$
$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0.$$

Let S_n be the A-submodule of $A[X]$ consisting of polynomials of degree $< n$. Choose bases B_1 (resp. B_2) of $S_m \times S_n$ (resp. S_{n+m}) by

$$B_1 = \{(X^{m-1}, 0), \dots, (X, 0), (1, 0), (0, X^{n-1}), \dots, (0, X), (0, 1)\}$$
$$(B_2 = \{X^{n+m-1}, \dots, X, 1\}).$$

Define an A-linear map $\phi : S_m \times S_n \to S_{n+m}$ by

$$\phi(u, v) = uf + vg.$$

Let us denote $R(f, g)$ the matrix of ϕ with respect to B_1 and B_2,

$$R(f,g) = \begin{pmatrix} a_n & a_{n-1} & \cdots & 0 & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \cdots & 0 \\ \dots & \dots & \ddots & \dots & \dots & \dots & \dots & 0 \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \cdots & \cdots & b_m & b_{m-1} & 0 & \cdots & b_0 \end{pmatrix}.$$

The square matrix $R(f, g)$ of size $(n+m)$ will be called the *resultant matrix* and the determinant of the resultant matrix $R(f, g)$ is called the *resultant* $\operatorname{res}(f, g)$ of f and g.

Now we state a main result of [3, Theorem 4.4] in the form we will use.

Theorem 2.1. *Let A be a Noetherian commutative ring and $f, g \in A[X]$ be monic polynomials of degree n and m respectively with $n > m$. Then $g(X)$ divides $f(X)$ if and only if the condition*

(R) *the minors of $R(f, g)$ of size bigger than n vanishes* *is satisfied.*

Remark. In (iv), of [3, Theorem 4.4] we may assume that a_n is a unit and the condition "the minors of $R(f,g)$ of size n generate the unit ideal" is redundant since the $n \times n$ matrix in the low left corner of $R(f,g)$ has determinant b_m^n is a unit already because we assumed a_n is a unit.

Let f, g be the monic polynomials

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0,$$
$$g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$$

over a commutative ring A with $n > m$. Let $t = (t_0, t_1, \dots, t_{m-1})$ be the variables and let

$$g_t(X) = X^m + t_{m-1}X^{m-1} + \cdots + t_0\ .$$

Let J, J' be subsets of $\{1, 2, \dots, m+n\}$ which consists of $n+1$ elements. Let $R(f,g)_{J,J'}$ be the submatrix of $R(f,g)$ comprised of j-th row and j'-th column for every $j \in J$ and $j' \in J'$. And let $\mu_{J,J'} = \det(R(f,g_t)_{J,J'})$. Notice that $\mu_{J,J'}$ always contains t_i's since $n > m$, i.e., $\mu_{J,J'}$ are polynomials in the variables $t_0, t_1, \dots, t_{m-1}$.

Corollary 2.2. *With the same notations of the theorem $f(X)$ is divisible by a polynomial of degree m if and only if the set of polynomials $\mu_{J,J'}(t_0,\ t_1, \dots,$ $t_{m-1})$ has a common solution $(b_0, b_1, \dots, b_{m-1})$. In this case,*

$$g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$$

divides the polynomial $f(X)$.

If A is a Noetherian domain, then we can simplify these polynomials. First we need a fact which probably is well known.

Lemma 2.3. *Let $F = A^n$ be the free module of rank n. Let $S = \{v_1, v_2, \dots, v_m\}$ $(m \leq n)$ be a set of vectors. Let M be the $m \times n$ matrix whose rows are $\{v_1, v_2, \dots, v_m\}$ and for $J \subset \{1, 2, \dots, n\}$ consisting of m elements, $M^{(J)}$ be the submatrix consisting of J-columns and μ_J be its determinant. Then S is linearly dependent if and only if the minors of size m of M are divisors of 0. That is there is λ such that $\lambda\mu_J = 0$ for all subset J of $\{1, 2, \dots, n\}$ consisting of m elements.*

Proof. Let $\{e_1, e_2, \dots, e_n\}$ be the standard basis of A^n. For a subset $J = \{j_1, j_2, \dots j_m\}$ of $\{1, 2, \dots, n\}$ we let $e_J = e_{j_1} \wedge e_{j_2} \cdots \wedge e_{j_m}$. By [1, Proposition 12, p. 519], $\{v_1, v_2, \dots, v_m\}$ is linearly dependent if and only if there is $\lambda \in A$ such that $\lambda v_1 \wedge v_2 \wedge \cdots \wedge v_m = 0$. But $v_1 \wedge v_2 \wedge \cdots \wedge v_m = \sum \mu_J e_J$. Since we know that $\{e_J\}_J$ is linearly independent we see that there is $\lambda \in A$ such that $\lambda v_1 \wedge v_2 \wedge \cdots \wedge v_m = 0$ if and only if $\lambda\mu_J = 0$ for all J. □

Corollary 2.4. *Let A be a Noetherian domain and $F = A^n$ be the free module of rank n. Then the set of row vectors $S = \{v_1, v_2, \ldots, v_m\}$ $(m \leq n)$ in F is linearly dependent if and only if the minors μ_J of size m of M vanish.*

Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ and $g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$ be monic polynomials $A[X]$ with $m < n$. Consider the submatrix of $R_L(f, g)$ which is the $(n+1) \times (n+m)$ matrix

$$R_L(f,g) = \begin{pmatrix} 0 & \cdots & 1 & a_{n-1} & & \cdots & \cdots & a_0 \\ 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 1 & b_{m-1} & 0 & \cdots & b_0 \end{pmatrix}$$

consisting of the last $n+1$ rows. For a subset J consisting of $n+1$ elements of $\{1, 2, \ldots, n+m\}$ let $R_L(f,g)^{(J)}$ be the $(n+1) \times (n+1)$ submatrix of $R_L(f,g)$ consisting of the columns $R_L(f,g)^{(j)}$ for $j \in J$.

Proposition 2.5. *Let A be a Noetherian domain and let f and g be as above. Then the polynomial f is divisible by the polynomial g of degree m if and only if the rows of $R_L(f,g)$ are linearly dependent.*

Proof. By Theorem 2.1, $g|f$ if and only if minors of size bigger than n vanish. Since the set of n vectors $\{R_{(m+1)}, R_{(m+2)}, \ldots, R_{(m+n)}\}$ is linearly independent, this is equivalent to that $\{R_{(m+1)}, R_{(m+2)}, \ldots, R_{(m+n)}\} \cup \{R_{(i)}\}$ is linearly dependent for some i $(1 \leq i \leq m)$ by Corollary 2.4. But obviously $R_{(i)}$ can be replaced by any $R_{(j)}$ $(1 \leq j \leq m)$. Hence this is equivalent to that $\{R_{(m+1)}, R_{(m+2)}, \ldots, R_{(m+n)}\} \cup \{R_{(m)}\}$ is linearly dependent; $R_L(f,g)$ is linearly dependent. □

Corollary 2.6. *With the same notation as in the proposition, we have $g|f$ if and only if all minors of $R_L(f,g)$ of size $n+1$ vanish.*

Now define

$$\mu_J(f, g_t) = \det R_L(f, g_t)_J$$

which is a polynomial in t_0, $t_1, \ldots, t_{m-1}$. Sometimes we will abbreviate $\mu_J(f, g_t) = \mu_J(f, m)$. There are $\binom{m+n}{n+1}$ such polynomials. We will show that when A is a Noetherian domain there is a polynomial $g(X) \in A[X]$ of degree m such that $g|f$ if and only if these polynomials have a common zero.

Theorem 2.7. *Let A be a Noetherian domain and let $f \in A[X]$ be a monic polynomial. Then the polynomial f has a divisor of degree m if and only if $\binom{m+n}{n+1}$ polynomials $\mu_J(f, m)$ have a common solution. If the polynomials $\mu_J(f, m)$ have a common solution $(t_0, t_1, \ldots, t_{m-1}) = (b_0, b_1, \ldots, b_{m-1})$, then $f(X)$ is divisible by $g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$.*

Proof. By Theorem 2.1, $g|f$ if and only if the condition (R) is satisfied. But by Corollary 2.4, this is equivalent to that $n+1$ rows of $R_L(f,g)$ are linearly dependent. Now this in turn is equivalent to that the determinants of the submatrices consisting of $n+1$ columns of $R_L(f,g)$ vanish. □

Corollary 2.8. *For a positive integer m $(m < n)$ if there is a subset J of $\{1, 2, \ldots, n+m\}$ consisting of m elements such that $\mu_J(f, m)$ has no solution, then $f(X)$ has no divisor of degree m.*

Corollary 2.9. *A polynomial $f(X) \in A[X]$ of degree n is irreducible if and only if for each m $(m < n)$ the polynomials $\mu_J(f, m)$, where J runs over all subsets of $\{1, 2, \ldots, n+m\}$ consisting of $n+1$ elements have no common solution.*

Corollary 2.10. *Let K be a field and $f, g \in K[X]$ be monic polynomials of degree n and m respectively with $n > m$. Then $g(X)$ divides $f(X)$ if and only if* $\operatorname{rank}(R_L(f,g)) = n$.

Proof. The condition (R) of Theorem 2.1 is equivalent to the fact that

$$\operatorname{rank}(R(f,g)) \le n.$$

However, the $n \times n$ matrix in the low left corner of $R(f,g)$ has nonzero determinant. □

Next we will give another point of view of this theorem. Let $R_{(i)}$ be the i-th row of $R_L(f,g)$ $(i = 1, 2, \ldots, n+1)$. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a monic polynomial. We have a map

$$\Phi_f : F^m \longrightarrow \bigwedge^m F^{n+m}$$

sending $(b_0, b_1, \ldots, b_{m-1})$ to $\sum_J \mu_J e_J = R_{(0)} \wedge R_{(1)} \wedge R_{(2)} \wedge \cdots \wedge R_{(n)}$, where $\mu_J = \det R_L(f,g)^{(J)}$ is the determinant of the matrix formed by the j-th columns for $j \in J$ which is a subset of $\{1, 2, \ldots, n+m\}$ consisting of $n+1$ elements. There are $\binom{m+n}{n+1}$ such terms. Then we can restate Theorem 2.7 as follows.

Theorem 2.11. *Let A be a Noetherian domain. Then a monic polynomial $f(X) \in A[X]$ of degree n has a divisor of degree m if and only if there is $(b_0, b_1, \ldots, b_{m-1}) \in A^m$ such that $\Phi_f(b_0, b_1, \ldots, b_{m-1}) = 0$.* □

3. Irreducibility of polynomials and Diophantine equations

In this section we find the Diophantine equations for a polynomial $f(X)$ over a Noetherian domain A whose existence of common solution is equivalent to the existence of a divisor of $f(X)$ with a certain degree.

For a positive integer m with $m < n$ consider the square matrix of size $(n - m + 1)$

$$W^{(f,m)} = \begin{pmatrix} -t_{m-1} & 1 & 0 & \cdots & & & & 0 \\ t_{m-2} & -t_{m-1} & 1 & 0 & 0 & & & 0 \\ -t_{m-3} & t_{m-2} & -t_{m-1} & 1 & 0 & & & 0 \\ \cdots & & \cdots & & & \cdots & & \\ (-1)^m t_0 & & \cdots & & & \cdots & & \\ 0 & \ddots & \cdots & & & \cdots & & \\ \vdots & \cdots & (-1)^m t_0 & \cdots & t_{m-2} & -t_{m-1} & 1 & 0 \\ 0 & \cdots & 0 & (-1)^m t_0 & \cdots & t_{m-2} & -t_{m-1} & 1 \\ (-1)^{n-m} a_m & \cdots & (-1)^{m+1} a_{n-m-1} & (-1)^m a_{n-m} & \cdots & a_{n-2} & -a_{n-1} & 1 \end{pmatrix}.$$

If we adopt the convention $t_k = 1$ when $k = m$ and $t_k = 0$ when $k > m$, then the (i, j)-th position of $W^{(f,m)}$ can be written succinctly

$$(W^{(f,m)})_{ij} = \begin{cases} (-1)^{i-j+1} t_{m+i-j+1} & (1 \le i \le n-m), \\ (-1)^{n-j} a_{m+j-1} & (i = n-m+1). \end{cases}$$

Let A_i $(i = 1, 2, \ldots, n-m)$ be the square submatrix of size $(n-m-i+2)$ on the lower right corner of $W^{(f,m)}$ and let $\alpha_i = |A_i|$. For example, $A_1 = W^{(f,m)}$, A_2 is the submatrix obtained by deleting the first row and the first column and A_3 is the submatrix obtained by deleting the first two rows and the first two columns etc. And lastly $A_{n-m} = \left(\begin{smallmatrix} -t_{m-1} & 1 \\ -a_{n-1} & 1 \end{smallmatrix}\right)$.

We have a set of polynomials in $t_0, \ldots, t_{m-1}$

$$\begin{cases} w_1^{(f,m)}(t_0, \ldots, t_{m-1}) & = a_0 - t_0|A_1|, \\ w_2^{(f,m)}(t_0, \ldots, t_{m-1}) & = a_1 - t_0|A_2| - t_1|A_1|, \\ & \cdots\cdots \\ w_{m-1}^{(f,m)}(t_0, \ldots, t_{m-1}) & = a_{m-2} - t_0|A_{m-1}| - t_1|A_{m-2}| - \cdots - t_{m-2}|A_1|, \\ w_m^{(f,m)}(t_0, \ldots, t_{m-1}) & = a_{m-1} - t_0|A_m| - t_1|A_{m-1}| - \cdots - t_{m-1}|A_1|. \end{cases}$$

Theorem 3.1. *Let A be a Noetherian domain. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ and $g(X) = X^m + b_{m-1}X^m + \cdots + b_0 \in A[X]$ with $(m < n)$. Then f is divisible by g if and only if $(b_0, b_1, \ldots, b_{m-1})$ is a solution to the system of equations*

$$\begin{cases} w_1^{(f,m)}(t_0, \ldots, t_{m-1}) = 0, \\ w_2^{(f,m)}(t_0, \ldots, t_{m-1}) = 0, \\ \qquad \cdots \\ w_m^{(f,m)}(t_0, \ldots, t_{m-1}) = 0. \end{cases}$$

As the proof of the theorem is rather complicated we give an example when f is a quartic and g is a quadratic.

Example 3.2. Let $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in K[X]$, where K is a field. Let $g(X) = X^2 + b_1X + b_0$. Then

$$R_L(f,g) = \begin{pmatrix} 0 & 1 & a_3 & a_2 & a_1 & a_0 \\ 1 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 1 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & 1 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & 1 & b_1 & b_0 \end{pmatrix}.$$

Now apply elementary row operations to get 0 on the 2,3 and 4-th positions of the first row and then interchange the rows to get

$$R_L \sim \begin{pmatrix} 1 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 1 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & 1 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & 1 & b_1 & b_0 \\ 0 & 0 & 0 & 0 & w_2 & w_1 \end{pmatrix}$$

(In the fifth row of the last matrix we interchanged w_1 and w_2 because the indices work better in that way). Then

$$\begin{cases} w_1 = a_0 - b_0(a_2 - b_0 - b_1(a_3 - b_1)) = a_0 - b_0\alpha_1, \\ w_2 = a_1 - b_0(a_3 - b_1) - b_1(a_2 - b_0 - b_1(a_3 - b_1)) = a_1 - b_0\alpha_2 - b_1\alpha_1, \end{cases}$$

where

$$\begin{cases} \alpha_2 = a_3 - b_1, \\ \alpha_1 = a_2 - b_0 - b_1\alpha_2. \end{cases}$$

If we let

$$W^{(f,2)} = \begin{pmatrix} -t_1 & 1 & 0 \\ t_0 & -t_1 & 1 \\ a_2 & -a_3 & 1 \end{pmatrix},$$

then $\alpha_2 = |A_2|(b_0, b_1)$, and $\alpha_1 = |A_1|(b_0, b_1)$. Finally

$$\begin{cases} w_1^{(f,2)}(t_0, t_1) = -t_0t_1^2 + a_3t_0t_1 + t_0^2 - a_2t_0 + a_0, \\ w_2^{(f,2)}(t_0, t_1) = -t_1^3 + a_3t_1^2 - a_2t_1 + 2t_0t_1 - a_3t_0 + a_1. \end{cases}$$

Hence $g(X) = X^2 + b_1X + b_0$ is a divisor of f if and only if (b_0, b_1) is a solution to the simultaneous equation $w_1^{(f,2)}(t_0, t_1) = 0, w_2^{(f,2)}(t_0, t_1) = 0$.

With this example in mind we give a proof of Theorem 3.1.

Proof. Consider

$$R_L(f,g) = \begin{pmatrix} 0 & \cdots & 1 & a_{n-1} & & \cdots & \cdots & a_0 \\ 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & & 1 & b_{m-1} & \cdots & b_0 \end{pmatrix}.$$

By adding a constant multiple of the rows $R_{(2)}, R_{(3)}, \dots, R_{(n-m+1)}$ to the first row successively we obtain a matrix of the form

$$R_L(f,g) \sim \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & w_m & \cdots & w_1 \\ 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 1 & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \cdots & \cdots & & 1 & b_{m-1} & \cdots & b_0 \end{pmatrix}.$$

Explicitly add $-R_{(m)}$ to $R_{(1)}$, add $-\alpha_{n-m}R_{(m-1)}$ to $R_{(1)}$ where $\alpha_{n-m} = a_{n-1} - b_{m-1}$; add $-\alpha_{n-m-1}R_{(m-2)}$ to $R_{(1)}$ where $\alpha_{n-m-1} = a_{n-2} - b_{m-2} - b_{m-1}\alpha_{n-m}$; add $-\alpha_{n-m-2}R_{(m-2)}$ to $R_{(1)}$ where $\alpha_{n-m-2} = a_{n-2} - b_{m-3} - b_{m-2}\alpha_{n-m} - b_{m-1}\alpha_{n-m-1}$ and so on. Then the first n entries of the first row becomes 0 and the next m positions become

$$\begin{aligned} w_1 &= a_0 - t_0\alpha_1, \\ w_2 &= a_1 - t_0\alpha_2 - t_1\alpha_1, \\ &\qquad \dots\dots \\ w_{m-1} &= a_{m-2} - b_0\alpha_{m-1} - b_1\alpha_{m-2} - \cdots - b_{m-2}\alpha_1, \\ w_m &= a_{m-1} - b_0\alpha_m - b_1\alpha_{m-1} - b_2\alpha_{m-2} - \cdots - b_{m-1}\alpha_1, \end{aligned}$$

where α's are defined inductively by

$$\begin{cases} \alpha_{n-m} & = a_{n-1} - b_{m-1}, \\ \alpha_{n-m-1} & = a_{n-2} - b_{m-2} - b_{m-1}\alpha_{n-m}, \\ \alpha_{n-m-2} & = a_{n-3} - b_{m-3} - b_{m-2}\alpha_{n-m} - b_{m-1}\alpha_{n-m-1}, \\ & \dots\dots \\ \alpha_{n-2m+1} & = a_{n-m} - b_0 - b_1\alpha_{n-m} - b_2\alpha_{n-m-1} - \cdots - b_{m-1}\alpha_{n-2m+2}, \\ \alpha_{n-2m} & = a_{n-m-1} - b_0\alpha_{n-m-1} - b_1\alpha_{n-m-2} - \cdots - b_{m-1}\alpha_{n-2m+1}, \\ & \dots\dots \\ \alpha_1 & = a_m - b_0\alpha_{m+1} - \cdots - b_{m-1}\alpha_2. \end{cases}$$

Next we need to show that $\alpha_i = |A_i|(b_0, b_1, \dots, b_{m-1})$. We prove this inductively

$$\alpha_{n-m} = a_{n-1} - b_{m-1} = \begin{vmatrix} -b_{m-1} & 1 \\ -a_{n-1} & 1 \end{vmatrix},$$

$$\alpha_{n-m-1} = a_{n-2} - b_{m-2} - b_{m-1}\alpha_{n-m} = \begin{vmatrix} -b_{m-1} & 1 & 0 \\ b_{m-2} & -b_{m-1} & 1 \\ a_{n-2} & -a_{n-1} & 1 \end{vmatrix}.$$

Here we expand the determinant according to the first column. In general, by a suitable change of indices it suffices to show that $\alpha_1 = |A_1|(b_0, b_1, \dots, b_{m-1})$, that is we need to show:

$$\alpha_1 = \begin{vmatrix} -b_{m-1} & 1 & 0 & \cdots & & & & 0 \\ b_{m-2} & -b_{m-1} & 1 & 0 & 0 & & & 0 \\ -b_{m-3} & b_{m-2} & -b_{m-1} & 1 & 0 & & & 0 \\ \cdots & & \cdots & & & \cdots & & \\ (-1)^m b_0 & & \cdots & & & \cdots & & \\ 0 & \ddots & \cdots & & & \cdots & & \\ \vdots & \cdots & (-1)^m b_0 & \cdots & b_{m-2} & -b_{m-1} & 1 & 0 \\ 0 & \cdots & 0 & (-1)^m b_0 & \cdots & b_{m-2} & -b_{m-1} & 1 \\ (-1)^{n-m} a_m & \cdots & (-1)^{m+1} a_{n-m-1} & (-1)^m a_{n-m} & \cdots & a_{n-2} & -a_{n-1} & 1 \end{vmatrix}$$

Expand the determinant according to the first column: Notice that when we delete the first column and the i-th row the resulting matrix is of the form

$$\begin{vmatrix} L & 0 \\ * & A_{i+1} \end{vmatrix},$$

where L is a lower triangular matrix with 1's on the diagonal. Hence, by induction

$$|A_1| = -b_{m-1}\alpha_2 - b_{m-2}\alpha_3 - \cdots - b_0\alpha_{m+1} + a_m. \qquad \square$$

Remark. If $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ and $g(X) = X + b_0$, then there is only one equation $w_1(t_0) = 0$. Now it can be easily checked that $w_1(-b_0) = f(-b_0)$. Hence $g|f$ if and only if $f(-b_0) = 0$ as it should be.

4. Irreducible quartic polynomials with rational coefficients

In this section we consider polynomials of degree 4 over a field. By using the results on the structure of rational points on some elliptic curves over $\mathbb{Q}$ we construct infinitely many irreducible quartic polynomials over $\mathbb{Q}$ which are not Einsensteinian.

First we recall some basic definitions of elliptic curves. See [2] for detail. An *elliptic curve* is given by a nonsingular homogeneous cubic equation

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

which is called the *Weierstrass equation*. It intersects with the line at infinity only at $(0,1,0)$. If $Z \neq 0$, then we divide the equation by Z^3 and let $x = X/Z$ and $y = Y/Z$ to obtain

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Now let $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$, a monic polynomial of degree 4 with rational coefficients. We know that f has a linear factor if and only if $f(X)$ has a root in $\mathbb{Q}$ which can be tested easily by evaluating at the possible roots of f.

In Example 3.2, if we replace $t_1 = y, t_0 = x$, then we obtain

$$\begin{cases} w_1^{(f,2)}(x,y) = -xy^2 + a_3xy + x^2 - a_2x + a_0, \\ w_2^{(f,2)}(x,y) = -y^3 + a_3y^2 - a_2y + 2xy - a_3x + a_1. \end{cases}$$

Hence by Theorem 3.1, $g(X) = X^2 + b_1X + b_0$ is a divisor of f if and only if (b_0, b_1) is a solution to the simultaneous equation $w_1^{(f,2)}(x, y) = 0, w_2^{(f,2)}(x, y) = 0$.

We look for the conditions on a_i's for which w_i $(i = 1, 2)$ has "no" solution. Then the quartics $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ will have no quadratic factor.

The structure or rational points of the elliptic curves

$$E_D : Y^2 = X^3 + DX$$

are relatively well known. And we check whether w_i can be reduced in this form. If the rational points of the elliptic curve corresponding to w_i are scarce and if they happen to be on the line at infinity, then we are able to find a family of irreducible quartics over $\mathbb{Q}$. We will show that for suitably chosen a's the cubic w_1 is of the form E_D. And when D is a prime which is congruent to $7, 11$ modulo 16 then it turns out that the only $\mathbb{Q}$ rational point on E_p are the 2-torsion points [2, p. 311].

Theorem 4.1. *Let E_p be the elliptic curve over $\mathbb{Q}$ defined by*

$$E_p \quad : \; y^2 = x^3 + px,$$

where $p \cong 7, 11 \pmod{16}$. Then the group $E_p(\mathbb{Q})$ of $\mathbb{Q}$-rational point of E_p is cyclic group of order 2 which is represented by $\{O, (0, 0)\}$.

Using this we will construct a 'family' of non-Eisensteinian irreducible quartics with rational coefficients. First we construct a family of rational quartics which do not have a quadratic factor.

Theorem 4.2. *Let p be an odd prime such that $p \cong 7, 11 \pmod{16}$. Then the quartics*

$$f(X) = X^4 + a_3X^3 + \frac{a_3^2}{4}X^2 + a_1X + \frac{1}{p^3} \qquad (a_1, a_3 \in \mathbb{Q})$$

has no quadratic factor.

Proof. Lets look at $w_1:$ We look for the case when w_1 has "no" solution so that we can get a family of quartics which is irreducible. If there is a solution (x, y) with $x = 0$, then $a_0 = 0$; $X|f(X)$, i.e., f is reducible. Hence we may assume $x \neq 0$. Homogenizing

$$W_1^{(f,2)}(X, Y, Z) = -XY^2 + a_3XYZ + X^2Z - a_2XZ^2 + a_0Z^3.$$

As $X \neq 0$ we let $y = Y/X$ and $z = Z/X$

$$w_1(y, z) = -y^2 + a_3yz + z - a_2z^2 + a_0z^3.$$

Now completing the square

$$w_1(y, z) = -\left(y - \frac{a_3}{2}z\right)^2 + z + \left(\frac{a_3^2}{4} - a_2\right)z^2 + a_0z^3.$$

If we let $t = y - \frac{a_3}{2}z$, $s = z$ and letting $w_1 = 0$ yields the equation

$$t^2 = s + c_1 s + c_2 s^3,$$

where $c_1 = (\frac{a_3^2}{4} - a_2)$ and $c_2 = a_0$. When $c_1 = 0$ the we are reduced to an elliptic curve of the form

$$Y^2 = X^3 + DX,$$

where $c_2 = a_0 = \alpha_0^3, \alpha_0 s = X, t = Y, D = \frac{1}{\alpha_0}$ [2, p. 309]. We know the rank and the torsion part and in some cases the torsion part is $\mathbb{Z}/2\mathbb{Z}$ and we can find the 2-torsion points $\{O, (0,0)\}$.

When D is a prime p with $p \cong 7, 11 \pmod{16}$. Then the group $E_p(\mathbb{Q})$ of $\mathbb{Q}$-rational point of E_p is cyclic group of order 2 which is represented by $\{O, (0,0)\}$. But the point O corresponds to $(X, Y, Z) = (0, 1, 0)$ which is on the line at infinity. Now the point $(0,0)$ corresponds to $(X, Y, Z) = (1, 0, 0)$ which is also on the line at infinity. Hence these two points do not give the solution to the equation $w_1 = 0$. □

Corollary 4.3. *Let p be an odd prime such that $p \cong 7, 11 \pmod{16}$. Then the quartics*

$$f(X) = X^4 + a_3 X^3 + \frac{a_3^2}{4} X^2 + a_1 X + \frac{1}{p^3} \qquad (a_1 \in \mathbb{Z}, a_3 \in 2\mathbb{Z}).$$

If $f(\frac{\pm 1}{p^i}) \neq 0$ $(i = 1, 2, 3)$, then f is irreducible.

Proof. Multiplying p^3 we get a polynomial of the form

$$h(X) = p^3 X^4 + c_3 X^3 + c_2 X^2 + c_1 X + 1 \qquad (c_i \in \mathbb{Z}).$$

It is well known that if $c = \frac{r}{s}$ $(r, s \in \mathbb{Z}, (r, s) = 1)$ is a root of $g(X)$, then $r = \pm 1$ and $s | p^3$. Hence our condition $f(\frac{\pm 1}{p^i}) \neq 0$ $(i = 1, 2, 3)$ guarantees that f has no root in $\mathbb{Q}$. Now by Theorem 4.2, f has no quadratic factor. Hence f is irreducible. □

5. Quintic polynomials with rational coefficients

We will have nothing much to say about the irreducibility of quintic polynomials. In this section, we simply make some random remarks on various possibilities for further study.

A monic quintic polynomial $f(X) = X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0 \in \mathbb{Q}[X]$ is irreducible if and only if f has no linear and quadratic factor. We can test whether f has a linear factor since we know how to find the possible root of f in $\mathbb{Q}$.

To see whether f has a quadratic factor $g(X) = X^2 + b_1 X + b_0$ consider

$$W^{(f,2)} = \begin{bmatrix} -t_1 & 1 & 0 & 0 \\ t_0 & -t_1 & 1 & 0 \\ 0 & t_0 & -t_1 & 1 \\ -a_2 & a_3 & -a_4 & 1 \end{bmatrix}.$$

Then we have

$$\begin{aligned} w_1^{(f,2)}(t_0,t_1) &= a_0 - t_0\alpha_0 \\ &= t_1^3t_0 - a_4t_1^2t_0 - 2t_1t_0^2 + a_3t_1t_0 + a_4t_0^2 - a_2t_0 + a_0, \\ w_2^{(f,2)}(t_0,t_1) &= a_1 - t_0\alpha_1 - t_1\alpha_0 \\ &= t_1^4 - a_4t_1^3 - 3t_1^2t_0 + a_3t_1^2 + a_4t_1t_0 - a_2t_1 + t_0^2 - a_3t_0 + a_1. \end{aligned}$$

Letting $y = t_1, x = t_0$ we have

$$\begin{cases} w_1(x,y) = y^4 - a_4y^3 - 3y^2x + a_3y^2 + a_4yx - a_2y + x^2 - a_3x + a_1, \\ w_2(x,y) = y^3x - a_4y^2x - 2yx^2 + a_3yx + a_4x^2 - a_2x + a_0. \end{cases}$$

Hence $f|g$ if and only if $w_i(b_0,b_1) = 0$ $(i = 1,2)$.

For example, if $a_4 = a_3 = a_2 = 0$ and $a_1 = a_0 = 1$; $f(X) = X^5 + X + 1$, then

$$\begin{cases} w_1(x,y) = y^4 - 3y^2x + x^2 + 1, \\ w_2(x,y) = y^3x - 2yx^2 + 1. \end{cases}$$

Now the equations $w_1 = 0, w_2 = 0$ have a common solution $x = 1, y = 1$ say by inspection. Hence $g(X) = X^2 + X + 1$ divides $f(X)$. In fact, $X^5 + X + 1 = (X^2 + X + 1)(X^3 - X^2 + 1)$. (To get the quotient upon dividing $f(X)$ by $g(X)$ we can use, of course, the long division of polynomials or we can use Theorem 4.4 of [3].) And it is a factorization into irreducible polynomials as can be easily checked.

Question 1. Can we find a family of irreducible quintics as we did for quartics?

Remark. As the degree of w_i is 4, we expect the genus of the corresponding curve is > 1. By Mordell's Conjecture proved by G. Faltings there ore only finitely many rational points. Hence we expect there are only finitely many rational solutions to $w_i = 0$ for each i. The existence or nonexistence of the common solution to the simultaneous equation $w_i = 0$ $(i = 1, 2, \dots, m)$ may be more difficult.

References

[1] N. Bourbaki, *Elements of Mathematics, Algebra I*, Addison-Wesley, 1973.

[2] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[3] S. S. Woo, *Dividing polynomials using the resultant matrix*, Comm. Algebra **35** (2007), no. 11, 3263–3272.

Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: sswoo@ewha.ac.kr