

Fatness of Polynomials over $Q(\sqrt{-m})$

Hiroshi IWATA

Introduction. Brown and Graham ([1]) introduced an idea “fatness” of polynomials over Z , to attain an irreducibility criterion for $P(x) \in Z[x]$.

The aim of this paper is to define the fatness $f = f(P) = f(P(x))$ for $P(x) \in R_m[x]$ in the similar way ($R_m =$ the integer ring of the field $k_m = Q(\sqrt{-m})$), to prove that

$f_m = \max_{P(x) \in R_m[x]} f(P)$ is a finite (natural) number and to give an irreducibility criterion for $P(x) \in R_m[x]$ by using f_m .

Preliminary description. If m runs through all natural numbers without essential square factors, k_m s exhaust all imaginary quadratic fields without repetition.

It is well known that R_m , $E_m =$ unit group of R_m and $D_m = \{\delta | \delta \in R_m \text{ and there exist two distinct elements } \alpha, \beta \in E_m \text{ with } \delta | \alpha - \beta\}$ are given concretely as follows:

$R_m = \{a + b\sqrt{-m} | a, b \in Z\}$ if $m \equiv 1, 2 \pmod{4}$, $= \{a + b(1 + \sqrt{-m})/2 | a, b \in Z\}$ if $m \equiv 3 \pmod{4}$,
 $E_1 = \{\pm 1, \pm i\} = \langle i \rangle$, $i = \sqrt{-1}$, $E_3 = \{\pm 1, \pm \omega, \pm \omega^2\} = \langle \omega \rangle$, $\omega = (1 + \sqrt{-3})/2$, $E_m = \{\pm 1\} = \langle -1 \rangle$ otherwise,
 $D_1 = \{\pm 1, \pm i, \pm 1 \pm i, \pm 2, \pm 2i\}$, $D_2 = \{\pm 1, \pm \sqrt{-2}, \pm 2\}$, $D_3 = \{\pm 1, \pm \omega, \pm \omega^2, \pm (1 + \omega), \pm \omega(1 + \omega), \pm \omega^2(1 + \omega), \pm 2, \pm 2\omega, \pm 2\omega^2\}$, $D_7 = \{\pm 1, (\pm 1 \pm \sqrt{-7})/2, \pm 2\}$ and $D_m = \{\pm 1, \pm 2\}$ if $m \neq 1, 2, 3, 7$.

Furthermore for $P(x) \in R_m[x]$, we shall define the following notations:

$d = d(P) = d(P(x)) =$ degree of $P(x)$, $p = p(P) = p(P(x)) = \{\alpha | \alpha \in R_m, P(\alpha) \neq 0 \text{ is indecomposable in } R_m\}^*$ (where $A^* =$ number of elements of a finite set A , and “ $\alpha \in R_m$ is indecomposable” means that if $\alpha = \beta\gamma$, $\beta, \gamma \in R_m$, then only one of β, γ lies in E_m), $u(P, \epsilon) = \{\alpha | P(\alpha) = \epsilon, \alpha \in R_m\}$ for $\epsilon \in E_m$, $u(P) = \{\alpha | P(\alpha) \in E_m, \alpha \in R_m\}^* = \sum_{\epsilon \in E_m} u(P, \epsilon)$, and finally we call $f = f(P) = f(P(x)) = u(P) - d(P)$ the fatness of $P(x)$ in $R_m[x]$, and call $P(x)$ fat when $f(P) \geq 1$.

From $P(x) \in R_m[x]$ we make $\epsilon_1 P(\epsilon_2 x + \beta)$ ($\epsilon_1, \epsilon_2 \in E_m$, $\beta \in R_m$) and $\bar{P}(x)$ (the polynomial with conjugate complex coefficients of corresponding coefficients of $P(x)$).

Repeating only finite times of these operations with all combinations of $\epsilon_1, \epsilon_2, \beta$ in arbitrary order, we obtain a subset $C(P(x))$ of $R_m[x]$. Obviously all operations are invertible, so that $C(P(x))$ is a classification of $R_m[x]$. It is clear that $P_1(x) \in C(P(x))$ implies $f(P_1(x)) = f(P(x))$. After the preparation we can describe our main theorem as

follows :

Main Theorem. Values of $f_m=2$, with two exceptions $f_1=4$, $f_3=5$.

(Then we can easily prove the following Theorem. $P(x) \in R_m[x]$ and $p(P(x))+2u(P(x)) > d(P(x))+2f_m$ implies the irreducibility of $P(x)$ in $R_m[x]$, by faithful tracing of Theorem in [1].)

Remark. The final aim of my study is perfect tracing of analogy of [1].

But the completion of classification of $R_m[x]$ and supplement of non-trivial numerical example as application of Theorem seem difficult. As I am obliged to omit a part of them, the writer wishes that the reader completes the incompleteness of this paper.

Proof of Main Theorem (1).

We assume $u(P,1)=\max_{\epsilon \in E_m} u(P,\epsilon)$ without loss of generality using $P(\epsilon x)$ in stead of $P(x)$.

Let $P(x)$ be a fat polynomial in $R_m[x]$ (there exists at least one fat polynomial in $R_m[x]$, as a fat polynomial in $Z[x]$ is always fat in $R_m[x]$ and $f_0 = \max_{P(x) \in Z[x]} f(P(x)) = 2$ (see [1])).

By the definition of $u(P,1)$, we get $P(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{u(P,1)})Q(x)+1$ (where $\alpha_1, \alpha_2, \cdots, \alpha_{u(P,1)}$ are distinct elements of R_m and $Q(x) \in R_m[x]$). For a fat $P(x)$, $0 < f(P(x)) = u(P(x)) - d(P(x)) = u(P,1) + \sum_{1 \neq \epsilon \in E_m} u(P,\epsilon) - (u(P,1) + d(Q(x))) = \sum_{1 \neq \epsilon \in E_m} u(P,\epsilon) - d(Q(x))$ and hence $\sum_{1 \neq \epsilon \in E_m} u(P,\epsilon) > d(Q(x)) = 0$. Thus let $P(\beta) = \epsilon \neq 1$. Then $(\beta - \alpha_1)(\beta - \alpha_2) \cdots (\beta - \alpha_{u(P,1)})Q(\beta) = -1 + \epsilon$. As $Q(x) \in R_m[x]$, $Q(\beta) \in R_m$ and $(\beta - \alpha_1)(\beta - \alpha_2) \cdots (\beta - \alpha_{u(P,1)}) \mid \epsilon - 1$.

(1) $m=1,2,3,7$. In this case $D_m = \{\pm 1, \pm 2\}$ and hence we have $u(P,1) \leq 3$.

(The product of suitably selected 3 distinct elements divides 2, but any products of 4 distinct elements of D_m does not.)

(The writer will describe our proof analytically and hope the reader to translate geometrically for smooth understanding.)

As is well known, any element of R_m is a vertex of the parallelogram generated from that with vertexes $0, 1, \sqrt{-m}, 1 + \sqrt{-m}$ (when $m \equiv 1, 2$) and $0, 1, (1 + \sqrt{-m})/2, (3 + \sqrt{-m})/2$ (when $m \equiv 3$). Let us notice that if geometrically $\beta_1, \beta_2, \cdots, \beta_{u(P,1)}$ is congruent to $\alpha_1, \alpha_2, \cdots, \alpha_{u(P,1)}$, so the polynomial obtained from $\beta_1, \beta_2, \cdots, \beta_{u(P,1)}$ by the operation mentioned hereafter is equivalent to what obtained from $\alpha_1, \alpha_2, \cdots, \alpha_{u(P,1)}$.

(11) When $u(P,1)=3$, we can assume $P(x)=(x^2-1)(x-2)(Q(x)+1, Q(x) \in R_m[x]$.

(In almost all cases the writer will select $P(x) \in C(P(x))$ as the set of β 's includes 0.)

(111) If $m \equiv 1, 2$, then $m \geq 5$ (as $m \neq 1, 2, 3, 7$) and $R = \{a + b\sqrt{-m} \mid a, b \in Z\}$. As $\beta \in Z$ implies $|\beta - 1|, |\beta + 1|, |\beta - 2| \geq \sqrt{5}$ and $|(\beta - 1)(\beta + 1)(\beta - 2)| \geq 5\sqrt{5}$ which contradicts to $(\beta - 1)(\beta + 1)(\beta - 2) \mid 2$, β must lie in Z . If $\beta \in Z$, then using $(\beta - 1)(\beta - 2)(\beta + 1) \neq 0$, we have

$\beta=0$, $u(P, -1)=1$, $4=u(P, 1)+u(P, -1)=u(P)>d(P)=3+d(Q)$ and $d(Q)=0$ successfully. As $Q(0)=-1$, we have $Q=-1$, $P(x)=-x^3+2x^2+x-1$. We see that $P(-x)=x^3+2x^2-x-1 \in C(P(x))$ is (c) in [1].

(112) If $m \equiv 3$, then $m \geq 11$. As $\beta \in Z$ implies $\min |\beta - a|^2 \geq ((1/2)^2 + (11/2)^2) = 3$ and hence $|(\beta-1)(\beta-2)(\beta+1)| = 3\sqrt{3} > 2$. Thus $P(\beta) = -1$ implies $\beta \in Z$ and by similar deduction to (111), we have $P(x) = x^3 + 2x^2 - x - 1$.

(Remark. Relation $(\beta-1)(\beta+1)(\beta-2) \mid 2$ implies $|\beta-1| |\beta+1| |\beta-2| \leq 2$ and hence in the complex plane, β lies in the meet of three discs $|\beta-1| \leq 2, |\beta-2| \leq 2, |\beta+1| \leq 2$ and hence we can find all β 's, by easy calculations of finite times. Therefore we will avoid hereafter redundant description for finding β 's.

(12) If $u(P, 1)=2$, then $(\beta - \alpha_1)(\beta - \alpha_2) \mid 2$ and $(\beta - \alpha_1, \beta - \alpha_2) = (1, -1), (1, 2), (1, -2), (-1, -2)$ or a transposition of each combination.

If necessary, adopting suitable $P_1(x) \in C(P(x))$ in stead of $P(x)$, we need only to consider the following (121) $P(x) = (x^2 - 1)Q(x) + 1$, (122) $P(x) = (x - 1)(x - 2)Q(x) + 1$, and (123) $P(x) = (x + 1)(x - 2)(Q(x) + 1)$.

In (121) $P(x) = (x^2 - 1)Q(x) + 1 = -1$ implies (omitting redundant explanation) $\beta = 0$, $d(Q) = 0$, $Q = 2$ and $P(x) = 2x^2 - 1$ ([1] (e)).

(122) $P(\beta) = -1$ implies $\beta = 0$, or 3, and $Q(0) = Q(3) = -1$. As $d(Q) < u(P, -1) = 2$, we have $d(Q) \leq 1$. Using $Q(0) = Q(3) = -1$, it follows $Q(x) = -1$, $P(x) = -x^2 + 3x - 1$ and $C(P(x)) \ni -P(-x+1) = x^2 + x - 1$ which is [1](b).

(123) $P(\beta) = -1$ implies $\beta = 0, 1$ and $Q(0) = Q(1) = 1$. As $u(P, -1) \leq 2$, we have $d(Q) \leq 1$ and hence $Q(x) = 1$, $P(x) = x^2 - x - 1$, $C(P(x)) \ni P(x+1) = x^2 + x - 1$ [1](b).

(13) $u(P, 1) = 1$ $P(x) = (x - 1)Q(x) + 1$, $u(P, -1) \leq u(P, 1) = 1$, $d(Q) = 0$ and $Q = \pm 2, \pm 1$ follows successfully. Thus we have (excluding equivalent polynomials) $P(x) = x$ or $2x - 1$ which are [1] (a) and (d).

If we define $F(P(x))$ by $(u(P, 1), u(P, -1), d(P), f(P))$, the following table will complete:

Representative of Class	F(P)=	u(P,1),	u(P,−1),	d(P),	f(P))
x		1,	1,	1	1
2x−1		1,	1,	1	1
2x ² −1		2,	1,	2	1
x ² +x−1		2,	2,	2	2
x ³ +2x ² −x−1		3,	1,	3	1

From this table we can learn that if $m \neq 1, 2, 3, 7$, we may select representative element of each equivalent class in $Z[x]$.

(2) $m = 2$ $E_2 = \{-1, 1\}$ $D_2 = \{\pm 1, \pm \sqrt{-2}, \pm 2\}$

For briefness, we describe hereafter as in the following (which will become shorter and shorter), but the reader may easily understand what is referred.

It is easy to prove $u(P, 1) \leq 4$.

(21) $u(P, 1) = 4$. $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\pm 1, \pm \sqrt{-2})$, $P(x) = (x^2 - 1)(x^2 + 2)Q(x) + 1$, $P(\beta) = -1$ implies $\beta = 0$, $Q = 1$, $P(x) = x^4 + x^2 - 1$ $F(P) = (4, 1, 4, 1)$.

(22) $u(P, 1) = 3$. $(\alpha_1, \alpha_2, \alpha_3) = (1, -1, 2), (1, -1, \sqrt{-2}), (1, \sqrt{-2}, -\sqrt{-2})$.

(221) $P(x) = (x^2 - 1)(x - 2)Q(x) + 1$, $\beta = 0$, $Q(x) = 1$, $P_1(x) = x^3 + 2x^2 - x - 1 \in C(P(x))$, $F(P) = (3, 1, 3, 1)$ [1](c).

(222) $P(x) = (x^2 - 1)(x - \sqrt{-2})Q(x) + 1$, $\beta = 0$, $Q(x) = \sqrt{-2}$, $P(x) = \sqrt{-2}x^3 + 2x^2 - \sqrt{-2}x - 1$, $(3, 1, 3, 1)$.

(223) $P(x) = (x^2 + 2)(x - 1) + 1$, $\beta = 0$, $Q = 1$, $P(x) = x^3 - x^2 + 2x - 1$ $(3, 1, 3, 1)$. (23) $u(P, 1) = 2$, $(\alpha_1, \alpha_2) = (1, -1), (1, \sqrt{-2}), (1, 2), (1, -2), (\sqrt{-2}, -\sqrt{-2})$.

(231) $P(x) = (x^2 - 1)Q(x) + 1$, $\beta = 0$, $Q = 2$, $2x^2 - 1$ $(2, 1, 2, 1)$.

(232) $P(x) = (x - 1)(x - \sqrt{-2})Q(x) + 1$, $\beta = 0$ or $1 + \sqrt{-2}$, $d(Q) \leq 1$, $Q(0) = Q(1 + \sqrt{-2}) = \sqrt{-2}$, $Q = \sqrt{-2}$. $P(x) = \sqrt{-2}x^2 + (2 - \sqrt{-2})x - 1$ $(2, 2, 2, 2)$.

From (233) and (234) we can lead to $x^2 + x - 1$ [1](b) as in (1).

(235) $P(x) = (x^2 + 2)Q(x) + 1$, $\beta = 0$, $P(x) = x^2 + 1$ $(1, 2, 1, 2)$.

(24) $u(P, 1) = 1$. We can easily obtain three inequivalent polynomials: x , $(1, 1, 1, 1)$, $2x - 1$, $(1, 1, 1, 1)$ $\sqrt{-2}x + 1$ $(1, 1, 1, 1)$.

Thus we have the following for $m = 2$:

$x^4 + x^2 - 1$	$(4, 1, 4, 1)$,	$x^3 + 2x^2 - x - 1$	$(3, 1, 3, 1)$,	$\sqrt{-2}x^3 + 2x^2 - \sqrt{-2}x - 1$	$(3, 1, 3, 1)$,
$x^3 - x^2 + 2x - 1$	$(3, 1, 3, 1)$,	$2x^2 - 1$	$(2, 1, 2, 1)$,	$\sqrt{-2}x + (2 - \sqrt{-2})x - 1$	$(2, 2, 2, 2)$,
$x^2 + x - 1$	$(2, 2, 2, 2)$,	$x^2 + 1$	$(1, 2, 1, 2)$,	$2x - 1$	$(1, 1, 1, 1)$,
$\sqrt{-2}x + 1$	$(1, 1, 1, 1)$,	x	$(1, 1, 1, 1)$.		

(3) $m = 7$, $E_7 = \{\pm 1\}$, $D_7 = \{\pm 1, \pm 2, \pm \alpha, \pm \bar{\alpha}\}$. $\alpha = (1 + \sqrt{-7})/2$, $u(P, 1) \leq 4$.

(31) $u(P, 1) = 4$. (311) $P(x) = x^4 - x^3 + x^2 + x - 1$, $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\pm 1, \alpha, \bar{\alpha})$, $(4, 1, 4, 1)$

(312) $P(x) = x^4 - \sqrt{-7}x^3 - 3x^2 + \sqrt{-7}x + 1$ $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\pm 1, \alpha, -\bar{\alpha})$, $(1, 4, 1, 4)$.

(32) $u(P, 1) = 3$, (321) $(\alpha_1, \alpha_2, \alpha_3) = (\pm 1, 2)$ $P(x) = x^3 + 2x^2 - x - 1$ [1](c). $(3, 1, 3, 1)$

(322) $(1, \alpha, \bar{\alpha})$ $P(x) = x^3 - 2x^2 + 3x - 1$ $(3, 1, 3, 1)$. (323) $(1, -\alpha, -\bar{\alpha})$ $x^3 + x - 1$ $(3, 1, 3, 1)$

(324) $(\pm 1, \alpha) - \bar{\alpha}x^3 - 2x^2 + \bar{\alpha}x - 1$ $(3, 1, 3, 1)$, (325) $(1, \alpha, -\bar{\alpha})$ $x^3 - (1 + \sqrt{-7})x^2 + (\sqrt{-7} - 2) + 1$, $(1, 3, 1, 3)$.

(33) $u(P, 1) = 2$. (331). $(1, -1)$ $2x^2 - 1$ $(2, 1, 2, 1)$, (332) $(1, -2)$ $x^2 + x - 1$, $(2, 2, 2, 2)$,

(333) $(1, \alpha) - \bar{\alpha}(x - 1)(x - \alpha) + 1$ $(2, 2, 2, 2)$. This polynomial $P(x)$ is equivalent to $Q(x) = \alpha(x - 1)(x + \bar{\alpha}) + 1$ with $(1, -\bar{\alpha})$ as $P(x) = -\bar{Q}(x - \alpha)$.

(334) $(1, 2)$ $x^2 - x + 1$ $(2, 2, 2, 2)$.

Here we wish to describe more precisely hoping to add a little explanation to other brief referring.

In this case $P(x) = (x-1)(x-2)Q(x) + 1$, and $P(\beta) = -1$ implies $\beta = 0, 3, \alpha, \bar{\alpha}$ ($\alpha = (1 + \sqrt{-7})/2$).

It follows at once that $d(Q(x)) \leq 3$. $P(\beta) = -1$ implies $Q(0) = Q(3) = -1$ and $Q(\alpha) = Q(\bar{\alpha}) = 1$. If $d(Q) = 0$, $\beta = 0, 3$ ($P(x) = -(x-1)(x-2) + 1$, $u(P, -1) = 2$, $f = 2$), or $\beta = \alpha, \bar{\alpha}$ ($P(x) = (x-1)(x-2) + 1$, $u(P, -1) = 2$, $f = 2$). If $d(Q) = 1$, putting $Q(x) = px + q$, we have $q = -1$ (1), $3p + q = -1$ (2), $\alpha p + q = 1$ (3) and $\bar{\alpha} p + q = 1$ (4). From (1) and (2), $p = 0$ results, contradicting to $d(Q) = 1$.

Assumption (3) and (4) produces the similar result. Adopting (1) and (3), we have $p = 2/\alpha = (3 - \sqrt{-7})/4 \in R_7$. In the case (1) and (4), (2) and (3), or (2) and (4) are similar. In the case $d(Q) = 2$, $Q(x) = px^2 + qx + r$, $Q(0) = r = -1$ (1), $Q(3) = 9p + 3q + r = -1$ (2), $Q(\alpha) = p\alpha^2 + q\alpha + r = 1$ (3) and $Q(\bar{\alpha}) = p\bar{\alpha}^2 + q\bar{\alpha} + r = 1$ (4). As $\alpha = (3 + \sqrt{-7})/2$, we have $p = \frac{1}{2} \notin R_7$ under the assumption (1), (2), (3), or (1), (2), (4). From (1), (3), (4), we are led to $p = -1/2$, also. Under (2), (3), (4), we have the similar result. Let $d(Q) = 3$, $Q(x) = px^3 + qx^2 + rx + s$. Then $Q(0) = -1$ (1), $Q(3) = 27p + 9q + 3r + s = -1$ (2), $Q(\alpha) = p\alpha^3 + q\alpha^2 + r\alpha + s = -1$, $Q(\bar{\alpha}) = p\bar{\alpha}^3 + q\bar{\alpha}^2 + r\bar{\alpha} + s = -1$. From (1), (2), we have $s = -1$, $r = -9p - 3q$. From these two equalities and (3), we have $p\alpha^3 + q\alpha^2 - (9p + 3q)\alpha = -2$. From (4) we have $p\bar{\alpha}^3 + q\bar{\alpha}^2 + r\bar{\alpha} = -2$. Adding and subtracting last two equalities, we have $-36p - 8q + 4 = -4p = 0$, contradicting to $d(Q) = 3$.

Thus have the table for $m = 7$ as follows :

Representative of class	$u(P, 1)$	$u(P, -1)$	$d(P)$	$f(P)$
$x^4 - x^3 + x^2 + x - 1$	4,	1,	4,	1,
$x^4 - \sqrt{-7}x^3 - 3x^2 + \sqrt{-7}x + 1$	1,	4,	1,	4,
$x^3 + 2x^2 - x - 1$	3,	1,	3,	1,
$x^3 - 2x^2 + 3x - 1$	3,	1,	3,	1,
$x^3 + x - 1$	3,	1,	3,	1,
$-\bar{\alpha}x^3 - 2x^2 + \bar{\alpha}x - 1$	3,	1,	3,	1,
$x^3 - (1 + \sqrt{-7})x^2 + (\sqrt{-7} - 2)x + 1$	1,	3,	1,	3,
$2x^2 - 1$	2,	1,	2,	1,
$x^2 + x - 1$	2,	2,	2,	2,
$x^2 - x + 1$	2,	2,	2,	2,
$-\bar{\alpha}(x-1)(x-\alpha) + 1$	2,	2,	2,	2,
$2x - 1$	1,	1,	1,	1,

$$\begin{array}{cccc} \alpha x + 1 & 1, & 1, & 1, & 1, \\ x & 1, & 1, & 1, & 1, \end{array}$$

By what is referred till here we have proved $f_m=2$ when $m \neq 1, 3$.

Let $m=1$. For $P(x)=(x-1)(x-2)+1$, $P(1+i)=P(2-i)=-i$, $P(1-i)=P(2+i)=i$ and $u(P,1)=2$, $u(P,i)=u(P,-i)=2$, $u(P) \geq 6$, $d(P)=2$ and $f(P) \geq 4$.

(1). If $\alpha_2, \alpha_2, \dots, \alpha_{u(P,1)}$ include $\pm 1, i$ (or three complex integers congruent to them), then β must be 0 (or corresponding value under the congruent transformation). (2). When $u(P,1)=5$, then $\alpha_1, \alpha_2, \dots, \alpha_{u(P,1)}$ must include $\pm 1, i$.

Thus if we seek $P(x)$ with $f(P) \geq 5$, we can assume that $u(P,1) \leq 4$.

(3). $u(P,1)=4$. We need to study only polynomials with β 's which does not include $\pm 1, i$. Then $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (31) (\pm 1, 1 \pm i), (32) (\pm 1, \pm(1+i)), (33) (\pm 1, +i \pm 1), (34) (1 \pm i, 1, i), (35) (1, i, \pm(1+i)), (36) (1, i, -i \pm 1), (37) (1, i, \pm(-1+i))$, and $\beta=0$ with exceptins $\beta=0$ and i in (33).

(4). $u(P,1)=3$. Then $(\alpha_1, \alpha_2, \alpha_3) = (41) (\pm 1, 2) (\beta=0), (42) (\pm 1, 2i) (\beta=0, i), (43) (i, \pm 1 + i) (\beta=0, 2i), (44) (1, i \pm 1), (\beta=0, i), (45) (1, \pm(1+i)), (\beta=0), (46) (\pm 1, 1+i), (\beta=0, i) (47) (1, i, 1+i) (\beta=0), (48) (1, i, 1-i) (\beta=0, 1+i), (49) (1, i, -1-i) (\beta=0)$. (5) $u(P,1)=2$. Then (51) $(\alpha_1, \alpha_2) = (1, 2) (\beta=0, 2 \pm i, 2 \pm i)$ and (52) $(1, -2) (\beta=0, -1), (53) (1, 2i) (\beta=0, i, 1+i, 1+2i), (54) (i \pm 1), (\beta=0, i, 2i), (55) (\pm(1+i) (\beta=0), (56) (1, i), (\beta=0, 1+i)$. (6) $u(P,1)=1$. In this case $u(P) \leq 4$, and hence $f(P) \leq 3$ as $d(P)=1$. As $f(P) \leq 4$ was known except $P(x)=(x-1)(x-2)Q(x)+1$, we need to study only this $P(x)$.

Let $P(x)=(x-1)(x-2)Q(x)+1$ with $Q(x) \in R[x]$. $Q(\beta)=-1$ implies $\beta=0, 3, 1 \pm i, 2 \pm i$, so that $u(P) \leq 8$. Therefore if we are interested only in $P(x)$ with $f(P) \geq 5$, we need only to study $P(x)$ with $d(P) \leq 3$ and hence $d(Q) \leq 1$. As $g(0)=g(3)=2$, $g(1+i)=g(2-i)=-(1+i)$, $g(1-i)=g(2+i)=-1+i$, when $g(x)=(x-1)(x-2)$, All possibilities are:

$P(0), P(3)=-1, Q(0), Q(3)=-1, P(1+i), P(2-i)=i, -i, -1, Q(1+i), Q(2+i)=-i, 1, 1-i, P(2+i), P(1-i)=i, -i, -1, Q(2+i), Q(1-i)=1, -i, 1+i$.

When $d(Q)=0$, $f(P)=4$. (Only 4 valnes $Q(0), Q(3), Q(2+i), Q(1-i)$ of values $Q(0), Q(3), Q(1+i), Q(2-i), Q(2+i), Q(1-i)$ can be $+1$. Similarly of these six values, only two can be -1 , and so on.

If $d(Q)=1$, then $u(P)=8$, and hence six values must lie in E . Thus we have $Q(0)=Q(3)=-1$, and $Q(x)=-1$ as $d(Q) \leq 1$, contradicting to $d(Q)=1$, which completes our proof when $m=1$.

Let $m=3$. If $u(P,1)=1$, then $f(P) \leq 5$ (and $f(P)=5$ when $P(x)=x$). If 4 elements of $\alpha_1, \alpha_2, \dots, \alpha_{u(P,1)}$ are on the unit circle, then $\beta=0$. (We need only to consider when the 4 elements are $(1, \omega, -1+\omega, -1), (1, \omega, \omega-1, -\omega)$ or $(\pm 1, \pm \omega)$, and we can verify

that $\beta=0$ in each case with ease).

If 3 elements are on the unit circle, then $f(P) \leq 4$. We can assume the 3 elements are $(1, \omega, \omega-1)$, $(1, \omega, -1)$ or $(1, \omega-1, -\omega)$. In each case $\beta=0$, $1+\omega, 2\omega-1$; $\beta=0$, $\omega-1$; $\beta=0, \omega, -1, 1-\omega$ respectively. If 2 elements are, we assume $(\alpha_1, \alpha_2) = (\omega, 1-\omega)$, $(1, -1)$ or $(\omega, \omega-1)$ with $\beta = (0, 1, \omega+1, \omega-1, -\omega, 2-\omega)$, $(\omega, \omega-1, -\omega, 1-\omega)$ $(-1, 0, 1, 2\omega, 2\omega-1, 2\omega-2)$ respectively.

Therefore on our standpoint to seek $P(x)$ with $f(P) \geq 6$, we need only to consider $u(P, 1) \leq 3$ and $(\alpha_1, \alpha_2) = (\omega, 1-\omega)$ or $(1, 2)$. Furthermore if we prove that there are no $P(x)$'s with $f(P) = 6$ when $u(P, 1) = 2$, $(\alpha_1, \alpha_2) = (\omega, 1-\omega)$ or $(1, 2)$, then it is clear there are no $P(x)$'s with $f(P) \geq 3$ and $u(P, 1) = 3$. Let $(\alpha, \beta) = (\omega, 1-\omega)$. There are just 6 β 's, we have $d(Q) = 0$. Calculating $h(x) = (x-\omega)(x-1+\omega)$ when $x = 0, 1, -1, \omega, \omega+1, \omega-1, 1-\omega, 2-\omega$, we obtain $P(0), P(1) = (\omega, \omega-1, -1, 1-\omega, -\omega)$ $Q(0), Q(1) = (\omega-1, \omega-2, -2, -\omega-1, -\omega)$, $P(\omega-1), P(2-\omega) = -1$, $Q(\omega-1), Q(2-\omega) = -\omega$, $P(\omega+1), P(-\omega) = -1$, $Q(\omega+1), Q(-\omega) = \omega-1$. This table shows that if $Q = -\omega$, $P(0) = P(1) = 1-\omega$, and $P(\omega-1) = P(2-\omega) = -1$, and if $Q = \omega-1$, then $P(0) = P(1) = \omega$, and $P(\omega+1) = P(-\omega) = -1$, Noticing that $-1, \pm(1-\omega) \in E_3$ when $P(x) = -\omega(x-\omega)(x+\omega-1)+1$ or $P(x) = (\omega-1)(x-\omega)(x+\omega-1)+1$, $f(P(x)) = 4$. For other choices of Q (mentioned above), we have $f(P(x)) = 2$. Finally let us study $P(x) = (x-1)(x-2)Q(x)+1$.

In this case β 's $= (0, 3, \omega-1, \omega, \omega+1, \omega+2, -\omega, -\omega+1, -\omega+2, -\omega+3)$. The following is obtained as often referred: $P(0), P(3) = -1$, $Q(0), Q(3) = -1$, $P(\omega), P(3-\omega) = (\omega-1, -\omega)$, $Q(\omega), Q(3-\omega) = (-\omega, 1-\omega)$, $P(1-\omega), P(\omega+2) = (\omega-1, -\omega)$, $Q(1-\omega), Q(\omega+2) = (\omega, \omega-1)$, $P(\omega+1), P(2-\omega) = (-1, \omega, -\omega, \omega-1, 1-\omega)$, $Q(\omega+1, 2-\omega) = (2, 1-\omega, 1+\omega, 2-\omega, \omega)$.

If $f(p) = u(P) - d(P) \geq 6$, then $10 = u(P) \geq d(P) + 6$, $d(P) \leq 4, d(Q) \leq 2$. When $f(P) = 6$, then $d(Q) = 0, 1, 2$ imply $d(P) = 2, 3, 4$ and $u(P) = 8, 9, 10$, respectively. If $d(Q) = 0$, then $f(P) = 6$ which is impossible.

(It is easily seen when we observe the table above).

If $d(Q) = 1$, then $d(P) = 3$, $u(P) = 9$. Then seven of above eight equalities must hold. $Q(0) = Q(3) = -1$ implies $Q = -1$ so that $d(Q) = 0$ contradicting to $d(Q) = 1$, Otherwise $Q(0) = -1$ and other six equalities hold or $Q(3) = -1$ and other six equalities hold. In the former case $Q(x) = bx - 1$, $b \in R_3$. As $Q(3-\omega) = 1-\omega$ or $-\omega$, we have $b = (1-\omega)/(3-\omega)$ or $(2-\omega)/(3-\omega)$, each of them is not in R_3 . As for $Q(3) = -1$ the proof is similar. If $d(Q) = 2$, then $d(P) = 4$, $u(P) = 10$. Putting $Q = px^2 + qx + r$, we have $r = -1$, $9p + 3q + r = -1$, so that $q = -3p$, $Q(x) = px^2 - 3px - 1$. As $Q(\omega) = -\omega$, or $1-\omega$, we have $p\omega^2 - 3p\omega - 1 = -\omega$, or $1-\omega$. Using $\omega^2 = \omega - 1$, we attain $(2\omega+1)p = \omega - 1$ or $\omega - 2$. But $N(2\omega+1) = 7$,

$N(1-\omega)=1$ and $N(2-\omega)=3$ show that $p \in R_3$. If $f=7$, then $d(Q)=0$, $u(P)=9$, or $d(Q)=1$, $u(P)=10$. If $f=8$, then $d(Q)=0$, $u(P)=10$.

They are impossible, and a proof is easier than above.

Reference

W.S. Brown and R.L. Graham An irreducibility Criterion for Polynomials over Integers, Amer. Math. Monthly, vol. 76(1969), 795-797.