On the finiteness of certain Rabinowitsch polynomials

Dongho Byeon

School of Mathematics, Korea Institute for Advanced Study, Seoul, Korea
e-mail: dhbyeon@kias.re.kr

and

H. M. Stark

Department of Mathematics, University of California, San Diego, CA, USA
e-mail: hmstark@ucsd.edu

Let m be a positive integer and $f_m(x)$ be a polynomial of the form $f_m(x) = x^2 + x - m$. We call a polynomial $f_m(x)$ a Rabinowitsch polynomial if for $t = [\sqrt{m}]$ and consecutive integers $x = x_0, x_0 + 1, \cdots, x_0 + t - 1$, $|f(x)|$ is either 1 or prime. In this note, we show that there are only finitely many Rabinowitsch polynomials $f_m(x)$ such that $1 + 4m$ is square free.

1 Introduction

In [**?**], Rabinowitsch proved the following theorem.

Theorem(Rabinowitsch) The class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{1-4m})$, $m \in \mathbb{N}$, is equal to 1 if and only if $x^2 - x + m$ is prime for any integer x such that $1 \leq x \leq m-2$.

In this paper, we shall consider an analogue of this for real quadratic fields. Let m be a positive integer and $f_m(x)$ be a polynomial of the form $f_m(x) = x^2 + x - m$. We call a polynomial $f_m(x)$ a Rabinowitsch polynomial if for $t = [\sqrt{m}]$ and consecutive integers $x = x_0, x_0 + 1, \cdots, x_0 + t - 1$, $|f(x)|$ is either 1 or prime. We shall prove the following theorems.

Theorem 1.1 *Every Rabinowitsch polynomial of the form $f_m(x) = x^2 + x - m$ is one of the following types.*

(i) $x^2 + x - 2$,

(ii) $x^2 + x - t^2$, *where t is 1 or a prime,*

(iii) $x^2 + x - (t^2 + t + n)$, *where $-t < n \leq t$ and where $|n|$ is 1 or $|n|=\frac{2t+1}{3}$ is an odd prime.*

Theorem 1.2 *If $f_m(x) = x^2 + x - m$ is a Rabinowitsch polynomial such that $K_m = \mathbb{Q}(\sqrt{1 + 4m})$ is a real quadratic field, then the class number of K_m is equal to 1.*

Theorem 1.3 *There are only finitely many Rabinowitsch polynomials $f_m(x) = x^2 + x - m$ such that $1 + 4m$ is square free.*

Remark. Similar results to Theorem 1.2 can be found in [**?**] or [**?**].

2 Proof of Theorem 1.1

It is obvious that $f_m(x)$ is a Rabinowitsch polynomial for $m = 1, 2, 4$ (for various choices of x_0). In what follows we exclude these cases. Then m is odd. For otherwise $f_m(x) = x^2 + x - m$ is even for all integers x. Therefore $f_m(x) = \pm 2$ for all integers x in the interval $[x_0, x_0 + t - 1]$ by definition of $f_m(x)$. This forces that $2(x_0 + 1) = f(x_0 + 1) - f(x_0) = \pm 4$ and $t = 2$. But this leads to $m = 4$.

Suppose that $m = t^2$ is an (odd) square. Then t divides some integer $x \in [x_0, x_0 + t - 1]$. It follows that t is a divisor of $f_m(x) = x^2 - x - t^2$ which, by definition, must be ± 1 or $\pm$ (prime). Thus t is 1 or a prime.

Suppose now that m is not a square. Write $m = t^2 + t + n$ for some (unique) integer n with $-t < n \leq t$. Since m is odd so is n. There is an integer $x \in [x_0, x_0 + t - 1]$ such that n divides $x - t$. Then n divides $f_m(x) = (x - t)(x + t + 1) - n$. By definition of $f_m(x)$ this forces that either $|n| = 1$ or $|n| = |f_m(x)|$ is an odd prime p. Assume the latter in what follows.

From $f_m(x) = n$ it follows that $(x-t)(x+t+1) = 2n$, which is impossible. Thus $f_m(x) = -n$ and $(x - t)(x + t + 1) = 0$. We conclude that either $x = t$ or $x = -t - 1$ is the unique integer in the interval $[x_0, x_0 + t - 1]$ satisfying the congruence $f(x) \equiv 0 \pmod{n}$. Both $x = t$ and $x = -t - 1$ satisfy this congruence, and if x satisfies it then also $x \pm n$. We infer that $p = |n|$ must be a divisor of $2t + 1 = t - (-t - 1)$ and that $\frac{t-1}{2} < p$. Write $p = \frac{2t+1}{k}$. Then $k \neq 1$ is an odd integer. For $k \geq 5$ one obtains $t < 7$ and $p < 3$, a contradiction. Thus $k = 3$ as desired. $\square$

Examples

(i) $m = 2$, $t = 1$, $x_0 = 0$.
(ii) $m = 169$, $t = 13$, $x_0 = 1$.
(iii)-1 $m = 1$, $t = 1$, $n = -1$, $x_0 = 0$.
(iii)-2 $m = 3$, $t = 1$, $n = 1$, $x_0 = 0$.
(iii)-3 $m = 103$, $t = 10$, $n = -7$, $x_0 = 4$.
(iii)-4 $m = 61$, $t = 7$, $n = 5$, $x_0 = 4$.

3 Proof of Theorem 1.2

Let $f_m(x) = x^2 + x - m$ be a Rabinowitsch polynomials such that $K_m = \mathbb{Q}(\sqrt{1 + 4m})$ is a real quadratic field. Let D_m denote the fundamental discriminant and M_{D_m} denote the Minkowski constant of the real quadratic field $K_m = \mathbb{Q}(\sqrt{1 + 4m})$, respectively. Then it is well known that $M_{D_m} = \frac{\sqrt{D_m}}{2}$ and the ideal class group of K is generated by prime ideals which lying over primes $l \leq M_{D_m}$. Thus to prove Theorem 1.2, it is enough to show that $(\frac{D_m}{2}) = -1$ and if $(\frac{D_m}{l}) = 0$ or 1 for a prime $2 < l \leq t = [\sqrt{m}]$, then (l) should be a product of two principal prime ideals.

We may assume that $m \neq 2, 4$ (as K_2 is not quadratic and $K_4 = \mathbb{Q}(\sqrt{17})$ has class number 1). Then m is odd (see Proof of Theorem 1.1) and so $D_m \equiv 1 + 4m \equiv 5 \pmod{8}$ (as $1 + 4m = u^2 D_m$ for some odd integer n). Thus $(\frac{D_m}{2}) = -1$.

Suppose now that $(\frac{D_m}{l}) = 0$ or 1 for a prime $2 < l \leq t$. Then there exist an integer $x \in [x_0, x_0 + t - 1]$ satisfying

$$(2x+1)^2 - (1+4m) \equiv 0 \mod l.$$

By the definition of $f_m(x)$, it should be that

$$(2x+1)^2 - (1+4m) = 4(x^2 + x - m) = \pm 4l.$$

Thus we have that

$$(l) = (\frac{(2x+1) + \sqrt{1+4m}}{2})(\frac{(2x+1) - \sqrt{1+4m}}{2})$$

which proves the theorem. □

4 Proof of Theorem 1.3

We only give the details of the case of type (iii) in Theorem 1.1. The other cases are trivial or similar to the case of type (iii).

Let $f_m(x) = x^2 + x - m$ be a Rabinowitsch polynomial of type (iii) and assume that $1 + 4m = (2t+1)^2 + 4n$ is square free. Then the real quadratic field $K_m = \mathbb{Q}(\sqrt{D_m})$, $D_m = (2t+1)^2 + 4n$, is of so-called Richaud-Degert type and its fundamental unit $\epsilon_m > 1$ is well known (see [?]):

$$\epsilon_m := \begin{cases} \frac{(2t+1)+\sqrt{(2t+1)^2+4n}}{2} & \text{if } |n| = 1 \\ \frac{2(2t+1)^2+4n}{|4n|} + \frac{2(2t+1)}{|4n|}\sqrt{(2t+1)^2+4n} & \text{if } |n| \neq 1. \end{cases}$$

The Siegel-Brauer theorem says that $\ln(R(D_m)h(D_m)) \sim \ln(\sqrt{D_m})$ as $D_m \to \infty$, where $R(D_m)$=lnϵ_m is the regulator and $h(D_m)$ is the class number of K_m. Thus Theorem 1.3 immediately follows from Theorem 1.2. □

Remark. For the present, it seems to be difficult to extend Theorem 1.3 to arbitrary $1 + 4m$.

ACKNOWLEDGMENTS

The authors would like to thank Mathematisches Forschungsinstitut Oberwolfach, Oberwolfach and Institute for Advanced Study, Princeton for giving them a chance to meet each other. The first author specially thanks the second author for suggesting this problem and giving outline of the proof. The authors also thanks the referee for many helpful suggestions.

References

[1] D. Byeon, A note on class number 1 criteria for totally real algebraic number fields, *Acta Arith.*, to appear.

[2] G. Degert, Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zhalkörper, *Abh. Math. Sem. Univ. Hamburg* **22** (1958), 92–97.

[3] M. Kutsuna, On a criterion for the class number of a quadratic number field to be one, *Nagoya Math. J.* **79** (1980), 123–129.

[4] G. Rabinowitsch, Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern, *J. reine angew. Math.* **142** (1913), 153–164.