C O L L O Q U I U M   M A T H E M A T I C U M

VOL. 122 2011 NO. 1

PRIME FACTORS OF VALUES OF POLYNOMIALS

BY

J. BROWKIN and A. SCHINZEL (Warszawa)

Abstract. We prove that for every quadratic binomial $f(x) = rx^2+s \in \mathbb{Z}[x]$ there are pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$, $f(a)$ and $f(b)$ have the same prime factors and $\min\{a, b\}$ is arbitrarily large. We prove the same result for every monic quadratic trinomial over $\mathbb{Z}$.

1. Introduction. Let $\mathcal{P}(n) = \{p \text{ prime} : p \mid n\}$. We study the problem when for a given polynomial $f \in \mathbb{Z}[x]$ there exist infinitely many pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$ and $\mathcal{P}(f(a)) = \mathcal{P}(f(b))$. For polynomials of degree one the question is easily answered by

THEOREM 1. *For all $r, s \in \mathbb{Z}$ there exists a strictly increasing sequence a_i of positive integers such that $\mathcal{P}(ra_i + s)$ is the same for all i.*

A related problem of whether $\mathcal{P}(a + i) = \mathcal{P}(b + i)$ $(i = 1, \dots, k)$ implies $a = b$ has been treated (see [1, Problem B29]).

For quadratic polynomials of non-zero discriminant an analogue of the above theorem is not true (by Pólya's theorem, the greatest prime factor of a value of such a polynomial tends to infinity with this value), and we only have

THEOREM 2. *For all $r, s \in \mathbb{Z}$, there exist pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$, $\mathcal{P}(ra^2 + s) = \mathcal{P}(rb^2 + s)$ and $\min\{a, b\}$ is arbitrarily large.*

THEOREM 3. *For every monic quadratic polynomial $f \in \mathbb{Z}[x]$ there exist pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$, $\mathcal{P}(f(a)) = \mathcal{P}(f(b))$ and $\min\{a, b\}$ is arbitrarily large.*

We have not been able to prove, even for $f(x) = x^2 - 1$, the existence of infinitely many triples $\langle a, b, c\rangle \in \mathbb{N}^3$ such that $a \neq b \neq c \neq a$ and $\mathcal{P}(f(a)) = \mathcal{P}(f(b)) = \mathcal{P}(f(c))$.

For polynomials of degree higher than two we know only numerical results communicated to us by J. Brzeziński and E. Reyssat. In particular, for $\max\{a, b\} \leq 4 \cdot 10^6$ and $n = 3$, and for $\max\{a, b\} \leq 10^4$ and $4 \leq n \leq 50$, there is only one pair $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$ and $\mathcal{P}(a^n - 1) = \mathcal{P}(b^n - 1)$, namely $\mathcal{P}(57^4 - 1) = \mathcal{P}(99^4 - 1)$.

2010 *Mathematics Subject Classification*: Primary 11N32; Secondary 11R11, 11R27.
Key words and phrases: values of polynomials, prime factors, non-singular quadratic units.

DOI: 10.4064/cm122-1-12

2. Proofs

Proof of Theorem 1. We can assume that $r > 0$. Let $d := (r, s)$. Then $f(x) = df_1(x)$, where $f_1(x) = r_1x + s_1$ and $(r_1, s_1) = 1$.

It follows that

$$\mathcal{P}(f(n)) = \mathcal{P}(d) \cup \mathcal{P}(f_1(n)) \quad \text{for every } n \in \mathbb{N}.$$

Take $m = r_1a_1 + s_1 > 1$. Then $(m, r_1) = 1$.

The Euler theorem gives, for every $i \in \mathbb{N}$,

$$m^{(i-1)\varphi(r_1)+1} = r_1(a_i - a_1) + m = r_1a_i + s_1 = f_1(a_i).$$

Hence

$$\mathcal{P}(f_1(a_i)) = \mathcal{P}(f_1(a_1)) = \mathcal{P}(m).$$

It follows that

$$\mathcal{P}(f(a_i)) = \mathcal{P}(m) \cup \mathcal{P}(d) \quad (i = 1, 2, \ldots). \ \blacksquare$$

Definition. Let $d \in \mathbb{N}$ be a non-square. We say that a unit $u + v\sqrt{d}$ of the order $\mathbb{Z}[\sqrt{d}]$ is *singular* if $(v, d) > 1$.

Let us remark that if the fundamental unit of the order $\mathbb{Z}[\sqrt{d}]$ is singular, then every unit of this order is singular.

Lemma. *Let $q, s \in \mathbb{Z}$, $q \neq 0$, $\varepsilon = \pm 1$. If there is a $k \in \mathbb{Z}$, $k \equiv \varepsilon \pmod{q}$, $(k, s) = 1$, such that $d := qs + k^2$ is positive, but not a square, and the fundamental unit η of the order $\mathbb{Z}[\sqrt{d}]$ is non-singular, then there are pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that $a \neq b$, $\mathcal{P}(qa^2 + s) = \mathcal{P}(qb^2 + s)$ and $\min\{a, b\}$ is arbitrarily large.*

Moreover, if qs is odd, a and b can be chosen odd.

Proof. In order to prove the first assertion of the lemma it suffices to find infinitely many pairs $\langle a, b\rangle \in \mathbb{N}^2$ such that

$$qa^2 + s = (qs + k^2)(qb^2 + s) \quad \text{and} \quad qs + k^2 \mid qb^2 + s.$$

Equivalently,

$$a^2 - db^2 = s \cdot \frac{d-1}{q} \quad \text{and} \quad d \mid qb^2 + s.$$

We have

$$N(1 + \sqrt{d}) = 1 - d, \qquad N(k - \varepsilon\sqrt{d}) = k^2 - d = -qs;$$

then

$$\alpha := (1 + \sqrt{d}) \cdot \frac{k - \varepsilon\sqrt{d}}{q} = \frac{k - \varepsilon d}{q} + \frac{k - \varepsilon}{q}\sqrt{d} \tag{1}$$

is in $\mathbb{Z}[\sqrt{d}]$ and satisfies $N(\alpha) = s \cdot \frac{d-1}{q}$. Therefore, it suffices to find infinitely many $n \in \mathbb{Z}$ such that

$$a + b\sqrt{d} := \alpha\eta^n \quad \text{satisfies} \quad d \mid qb^2 + s, \quad \text{or equivalently} \quad d \mid q^2b^2 - k^2.$$

Let $I := d\,\mathbb{Z}[\sqrt{d}]$ be the ideal of the ring $\mathbb{Z}[\sqrt{d}]$ generated by d. Then

$$\eta^n = (u + v\sqrt{d})^n \equiv u^n + nu^{n-1}v\sqrt{d} \pmod{I},$$

hence

$$\begin{aligned}\alpha\eta^n q &\equiv (k + (k-\varepsilon)\sqrt{d})(u^n + nu^{n-1}v\sqrt{d})\\ &\equiv u^{n-1}(ku + ((k-\varepsilon)u + nkv)\sqrt{d}) \pmod{I}.\end{aligned}$$

Therefore,

$$qa \equiv ku^n \pmod{d}, \tag{2}$$

$$qb \equiv u^{n-1}((k-\varepsilon)u + nkv) \pmod{d}. \tag{3}$$

From $u^2 - dv^2 = N(\eta)$ we obtain $u^2 \equiv N(\eta) \pmod{d}$, hence

$$q^2b^2 \equiv N(\eta)^{n-1}((k-\varepsilon)u + nkv)^2 \pmod{d}. \tag{4}$$

Therefore $q^2b^2 \equiv k^2 \pmod{d}$ holds provided

$$n \equiv 1 \pmod{2}, \qquad (k-\varepsilon)u + nkv \equiv k \pmod{d}. \tag{5}$$

There are infinitely many n satisfying this system of congruences, since $(kv, d) = 1$ and if $d \equiv 1 \pmod{2}$ the Chinese Remainder Theorem applies, while if $d \equiv 0 \pmod{2}$ then $k \equiv 1 \pmod{2}$ and the congruences in question are compatible.

In order to prove the second assertion of the lemma we notice that if $k \equiv 1 \pmod{2}$, then $d \equiv 0 \pmod{2}$, hence $uv \equiv 1 \pmod{2}$ and, by (2)–(5), $ab \equiv 1 \pmod{2}$.

If $k \equiv 0 \pmod{2}$, then $d \equiv 1 \pmod{2}$, hence, by (1), $\alpha \equiv 1+\sqrt{d} \pmod{2}$. Also $\eta^n = u_n + v_n\sqrt{d}$, where $u_n + v_n \equiv 1 \pmod{2}$, hence

$$a + b\sqrt{d} \equiv (1+\sqrt{d})(u_n + v_n\sqrt{d}) \equiv 1 + \sqrt{d} \pmod{2}$$

and $ab \equiv 1 \pmod{2}$. ∎

Proof of Theorem 2. We may assume $rs \neq 0$. Put

$$w = 900rs + 1, \qquad p = \frac{w^2-1}{4}$$

and take in the Lemma

$$q = 900r(w+2)^2, \qquad k = pqs + 1.$$

Hence

$$d = qs + k^2 = p^2q^2s^2 + (2p+1)qs + 1 = \frac{w^2}{4p^2}\left(\left(\frac{2p^2qs + 2p + 1}{w}\right)^2 - 1\right).$$

We have $8(2p^2qs+2p+1) \equiv 15w^2 \pmod{w^3}$, and since w is odd and $|w| > 1$,

$$\frac{2p^2qs + 2p + 1}{w^2} \in \mathbb{Z}, \qquad \left|\frac{2p^2qs + 2p + 1}{w}\right| > 1, \qquad d > 0,\ d \neq \square.$$

In the order $\mathbb{Z}[\sqrt{d}]$ there is a non-singular unit

$$\eta = \left(\frac{2p^2qs+2p+1}{w}\right)^2 + \frac{d}{w^2}\cdot 4p^2 + \sqrt{d}\cdot 4p\cdot\frac{2p^2qs+2p+1}{w^2} = \zeta^2,$$

where

$$\zeta = \frac{2p^2qs+2p+1}{w} + 2p\sqrt{\frac{d}{w^2}}$$

is a unit of $\mathbb{Z}[\sqrt{d/w^2}]$ and, since $(w,15)=1$,

$$\left(\frac{2p^2qs+2p+1}{w^2}, w\right) = 1.$$

Hence, by the lemma, there exist pairs $\langle a,b\rangle \in \mathbb{N}^2$ such that $a \neq b$, $\mathcal{P}(qa^2+s) = \mathcal{P}(qb^2+s)$ and $\min\{a,b\}$ is arbitrarily large.

Since $qa^2 = r(30(w+2)a)^2$, $qb^2 = r(30(w+2)b)^2$ and $w \neq -2$, the theorem follows. ∎

Proof of Theorem 3. Applying, if necessary, an integral translation of x we may assume that $f(x) = x^2+s$ or x^2+x+t. In the first case we apply Theorem 2.

In the second case we apply the second assertion of the Lemma with $q=1$, $s=4t-1$ and $k=2$ if $t=0$, $k=t-1$ if $t\neq 0$, $t\equiv 0 \pmod 3$, and $k=3t-1$ if $t\not\equiv 0 \pmod 3$. In the order $\mathbb{Z}[\sqrt{d}]$ there is a non-singular unit $2+\sqrt{3}$, $t+1+\sqrt{d}$ and $9t-1+3\sqrt{d}$, respectively.

We infer the existence of a,b odd such that $a\neq b$, $\mathcal{P}(a^2+s) = \mathcal{P}(b^2+s)$ and $\min\{a,b\}$ is arbitrarily large. Taking $a = 2a_1+1$, $b = 2b_1+1$ we conclude that $\mathcal{P}(4f(a_1)) = \mathcal{P}(4f(b_1))$. Since $f(a_1)\equiv t\equiv f(b_1) \pmod 2$, the last equality implies $\mathcal{P}(f(a_1)) = \mathcal{P}(f(b_1))$. ∎

REFERENCES

[1] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2005.

J. Browkin, A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: browkin@impan.pl
schinzel@impan.pl

Received 4 August 2010;
revised 3 November 2010 (5411)