МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2003
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2003
Proceedings of the Thirty Second Spring Conference of
the Union of Bulgarian Mathematicians
Sunny Beach, April 5–8, 2003

ON THE UNICITY CONJECTURE FOR THE HURWITZ EQUATION

Kaloyan St. Slavov

We prove the unicity conjecture for Markoff numbers which are powers of primes. We consider the corresponding conjecture for the Hurwitz equation and prove it assuming some natural restrictions.

1. Introduction. We shall use tools from algebraic number theory to analyze some properties of the solutions of Markoff's equation

$$x^2 + y^2 + z^2 = 3xyz \tag{1}$$

and some of its generalizations. Equation (1) appeared in approximation theory and was solved by Markoff using elementary methods only [5]. See [4] for a sketch of the original proof of Markoff.

If (x, y, z) is a solution of (1) in integers, we assume that $1 \leq x \leq y \leq z$. The number z is called a *Markoff number*. In 1913 Frobenius [2] stated his *unicity conjecture*, namely that there do not exist two distinct solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) of (1) such that $z_1 = z_2$. Baragar [1] proved that the unicity conjecture is true for prime Markoff numbers. He also established that the unicity conjecture is true if one of the numbers m, $3m-2$, or $3m+2$ is prime, twice a prime, or four times a prime. Based on the paper by Baragar, we generalize this result and prove that the unicity conjecture is true for Markoff numbers which are powers of primes. We consider a similar question for the more general Hurwitz equation [3]

$$x_1^2 + x_2^2 + \cdots + x_n^2 = Ax_1x_2\ldots x_n \tag{2}$$

in the special case $A = n$. Namely, we prove that there do not exist two distinct solutions $(x_1', x_2', x_3, \ldots, x_n)$ and $(x_1'', x_2'', x_3, \ldots, x_n)$ of (2) satisfying $0 < x_1' < x_2' < x_n$ and $0 < x_1'' < x_2'' < x_n$ if some natural restrictions on the numbers $x_3, \ldots, x_n$ hold.

The main idea of our proof for the unicity conjecture is to leave the ring $\mathbb{Z}$ and to consider an order in an appropriately chosen number field. The proof is based on the interpretation of the equation under consideration as a norm equation in this order. To complete the proof, we use the uniqueness of the factorization of given ideals as a product of prime ideals.

2. Elementary results for the Hurwitz equation. In this section we state some elementary facts concerning the Hurwitz equation which will be applied later in the proof of the main results. See [3] for the general case and [5] (and also [4]) for the case $n = 3$.

We shall consider equations of the type (2). The n-vector $(0, 0, \ldots, 0)$ is a solution of this equation. If $(x_1, x_2, \ldots, x_n)$ is a solution of (2), $x_i \neq 0$ for $i = 1, 2, \ldots, n$ and

$x_1 < 0$, then at least one more number x_j in the set $\{x_2, x_3, \dots, x_n\}$ is negative. If we replace x_1 by $-x_1$ and x_j by $-x_j$, we shall obtain a solution of (2) with fewer negative coordinates. Therefore, we may consider equations of the type (2) in positive integers only. The description of the solutions of (2) is the following.

Theorem 1. *The set $S \subset \mathbb{Z}^n$ of all solutions $(x_1, x_2, \dots, x_n)$ in positive integers of the equation*

$$x_1^2 + x_2^2 + \dots + x_n^2 = n x_1 x_2 \dots x_n, \tag{3}$$

satisfying $1 \le x_1 \le x_2 \le \dots \le x_n$ is the minimum set with the following properties:

- $(1, 1, \dots, 1) \in S$;
- *If $(x_1, x_2, \dots, x_n) \in S$ and $1 \le i \le n-1$ then*

  $$(x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_n, n x_1 \dots x_{i-1} x_{i+1} \dots x_n - x_i) \in S. \tag{4}$$

  The vector (4) has a greater last coordinate than the vector $(x_1, x_2, \dots, x_n)$.

Theorem 2. *The equation $x_1^2 + x_2^2 + \dots + x_n^2 = A x_1 x_2 \dots x_n$ has no solutions in positive integers if $A > n$ is an integer.*

Lemma 3. *If (x, y, z) is a solution of Markoff's equation (1) in positive integers then x, y, z are pairwise coprime.*

3. The main results

3.1. The conjecture for the Hurwitz equation. We shall interpret the equation (2) in the case $A = n$ as a norm equation in a certain order of an appropriately chosen quadratic field. We look at the unique factorization of certain ideals of this order. Lemma 5 below gives us some information about this factorization.

Let $m_1, m_2, \dots, m_k$, $m_1 \le m_2 \le \dots \le m_k$ be fixed positive integers with the following properties:

1. If k is odd, then all numbers m_i, $i = 1, 2, \dots, k$, are also odd;
2. $m_1^2 + m_2^2 + \dots + m_k^2 = p$ or p^2 for some prime number $p \in \mathbb{Z}$.
3. $p \nmid D$, where

$$D = \begin{cases} \frac{(k+2)^2}{4} m_1^2 m_2^2 \dots m_k^2 - 1, & \text{if } k \text{ is even} \\ (k+2)^2 m_1^2 m_2^2 \dots m_k^2 - 4, & \text{if } k \text{ is odd.} \end{cases}$$

We examine the number of the solutions (x, y) of the equation

$$x^2 + y^2 + m_1^2 + m_2^2 + \dots + m_k^2 = (k+2) m_1 m_2 \dots m_k x y, \tag{5}$$

satisfying the condition $0 < x < y < m_k$.

Let us assume that $p \neq 2$. We define

$$\omega = -\frac{(k+2)}{2} m_1 m_2 \dots m_k + \begin{cases} \sqrt{D}/2, & \text{if } k \text{ is odd} \\ \sqrt{D}, & \text{if } k \text{ is even.} \end{cases}$$

We write D in the form $D = f^2 d$ where d is square-free. If we assume that $d = 1$, we would have $u^2 - f^2 = 1$ or $u^2 - f^2 = 4$ for some $u \in \mathbb{N}$ according to whether D is even or odd, which is impossible. We consider the real quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ with ring of integers $\mathcal{O}_{\mathcal{K}}$. Let $\mathcal{R} = \mathbb{Z} + \omega\mathbb{Z} = \{a + \omega b \,|\, a, b \in \mathbb{Z}\}$. We recall that an order of $\mathcal{O}_{\mathcal{K}}$ is a set $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_{\mathcal{K}} = \{z + f\alpha | z \in \mathbb{Z}, \alpha \in \mathcal{O}_{\mathcal{K}}\}$, where f is a fixed positive integer. The number f is called the conductor of the order $\mathcal{O}_f$.

Lemma 4. *The set $\mathcal{R}$ is an order of $\mathcal{O}_{\mathcal{K}}$ of conductor f.*

Proof. We shall consider cases depending on the residue of k modulo 4.

1) $k = 2n-1$, $n \in \mathbb{N}$. Then $D = (2n+1)^2 m_1^2 m_2^2 \dots m_k^2 - 4 = f^2 d$. Hence, $D \equiv 1 \pmod 4$, f is odd, $f^2 \equiv 1 \pmod 4$ and thus $d \equiv 1 \pmod 4$. Therefore, the ring of integers of $\mathcal{K}$ is $\mathcal{O}_{\mathcal{K}} = \mathbb{Z} + \mathbb{Z}\frac{(1+\sqrt{d})}{2}$ and $\omega = -\frac{(k+2)}{2} m_1 m_2 \dots m_k + \frac{\sqrt{D}}{2} = \frac{a}{2} + \frac{\sqrt{D}}{2}$ where a is odd. Now, the equality $\mathbb{Z} + \omega\mathbb{Z} = \mathbb{Z} + f\mathcal{O}_{\mathcal{K}}$ follows from $p + q(\frac{a}{2} + \frac{f\sqrt{d}}{2}) = p + q\frac{(a-f)}{2} + fq\frac{(1+\sqrt{d})}{2}$ and $x + f(y + q\frac{(1+\sqrt{d})}{2}) = x + fy + q\frac{(f-a)}{2} + q(\frac{a}{2} + \frac{f\sqrt{d}}{2})$ (the number $(f-a)$ is even).

2) The proof in each of the cases $k = 4n+2$ and $k = 4n$ is similar to that in the case $k = 2n-1$. $\square$

Lemma 5. *Let (x, y) be a solution of (5), such that $0 < x < y$. Let $\beta = x + \omega y \in \mathcal{R}$. The ideal (β) is primitive, i.e., there does not exist $n \in \mathbb{Z}$, $n \neq 0, \pm 1$, such that $(\beta) = (n)I$ for some ideal $I \subseteq \mathcal{R}$, and the same holds for the ideal $(\overline{\beta})$.*

Proof. Let us assume that Lemma 5 is not true. It would follow that $\beta = nl$ for some $l = a + \omega b \in I$, which implies $x = na$, $y = nb$. To get a contradiction, it is enough to show that $\gcd(x, y) = 1$. If we assume that there is a prime $q \in \mathbb{Z}$, $q|x$, $q|y$, then (5) implies $q^2 | (m_1^2 + m_2^2 + \dots + m_k^2)$. Thus $\sum_{i=1}^k m_i^2 = p^2$ and $q = p$. Let $x = px_1$, $y = py_1$ for some integers x_1, y_1. The equation (5) implies $x_1^2 + y_1^2 + 1 = ((k+2)m_1 m_2 \dots m_k).x_1.y_1.1$ which is a contradiction to Theorem 2. $\square$

Theorem 6. *There is at most one pair $\{(\beta), (\overline{\beta})\}$ of principal ideals of $\mathcal{R}$ satisfying $N(\beta) = -m_1^2 - m_2^2 - \dots - m_k^2$.*

Proof. Let $\beta = x + \omega y$. We check that $N(\beta) = N(x + \omega y) = x^2 + y^2 - (k + 2)m_1 m_2 \dots m_k xy$ and rewrite the equation (5) as

$$N(\beta) = -m_1^2 - m_2^2 - \dots - m_k^2. \tag{6}$$

We have that

$$\operatorname{disc}(\mathcal{R}) = f^2 \operatorname{disc}(\mathcal{K}) = \begin{cases} D, & \text{if } \operatorname{disc}(\mathcal{K}) = d \\ 4D, & \text{if } \operatorname{disc}(\mathcal{K}) = 4d. \end{cases}$$

Since p is an odd prime number, Condition 3 implies $\gcd(N((\beta)), \operatorname{disc}(\mathcal{R})) = 1$. Hence the principal ideal $(\beta) \subseteq \mathcal{R}$ factors uniquely as a product of prime ideals of $\mathcal{R}$. Since $N(\beta) = \beta\overline{\beta}$, we know that

$$(\beta)(\overline{\beta}) = (N(\beta)) = (-m_1^2 - m_2^2 - \dots - m_k^2) = (m_1^2 + m_2^2 + \dots + m_k^2) = \begin{cases} (p) \\ (p)^2. \end{cases}$$

Since $p \in \mathbb{Z}$ is a prime number, $p \nmid \operatorname{disc}(\mathcal{R})$, (p) factors uniquely as a product of prime ideals of $\mathcal{R}$. Furthermore, either $(p) = P\overline{P}$, where $P \subseteq \mathcal{R}$ is a prime ideal or (p) is a prime ideal of $\mathcal{R}$. Therefore,

$$(\beta)(\overline{\beta}) = \begin{cases} P\overline{P} & \text{for some prime ideal } P \subseteq \mathcal{R} \\ P^2\overline{P}^2 & \text{for some prime ideal } P \subseteq \mathcal{R} \\ (p) \\ (p)^2. \end{cases}$$

According to Lemma 5, the last two cases of the factorization of $(\beta)(\overline{\beta})$ are impossible, because the prime ideal (p) appears as a factor either of (β) or $(\overline{\beta})$, but both of them are primitive.

Therefore, $(\beta)(\overline{\beta}) = \begin{cases} P\overline{P} \\ P^2\overline{P}^2. \end{cases}$

Since $P\overline{P} = (p)$, only one of the ideals P, $\overline{P}$ can appear in the factorization of (β) and the same is true for $(\overline{\beta})$ (according to Lemma 5). Therefore, in the first case we have that $\{(\beta), (\overline{\beta})\} = \{P, \overline{P}\}$ and in the second case we have $\{(\beta), (\overline{\beta})\} = \{P^2, \overline{P}^2\}$.

We showed that the pair $\{(\beta), (\overline{\beta})\}$ of principal ideals satisfying $N(\beta) = -m_1^2 - m_2^2 - \cdots - m_k^2$ is determined uniquely, because the pair of ideals $\{P, \overline{P}\}$ is determined uniquely by the unique factorization of the ideal $(p) \subseteq \mathcal{R}$. $\square$

The proof of the main result (Theorem 8) is based on the following interpretation of the unicity conjecture:

Theorem 7. *If there is at most one pair $\{(\beta), (\overline{\beta})\}$ of principal ideals of $\mathcal{R}$ satisfying $N(\beta) = -m_1^2 - m_2^2 - \cdots - m_k^2$, then there is at most one integer solution (x, y) of the equation* (5) *satisfying $0 < x < y < m_k$.*

We shall not give the proof of this result because it is technical and follows the idea in [1]. Together with the result of Theorem 6 (since the case $p = 2$ is trivial by Condition 2), this proves the main result:

Theorem 8. *Let $m_1, m_2, \ldots, m_k$, $m_1 \le m_2 \le \cdots \le m_k$ be fixed positive integers with the following properties:*

1. *If k is odd, then all numbers m_i, $i = 1, 2, \ldots, k$, are odd;*
2. *$m_1^2 + m_2^2 + \cdots + m_k^2 = p$ or p^2 for some prime number $p \in \mathbb{Z}$.*
3. *$p \nmid D$, where*

$$D = \begin{cases} \frac{(k+2)^2}{4} m_1^2 m_2^2 \ldots m_k^2 - 1 & \text{if } k \text{ is even} \\ (k+2)^2 m_1^2 m_2^2 \ldots m_k^2 - 4 & \text{if } k \text{ is odd.} \end{cases}$$

Then the equation

$$x^2 + y^2 + m_1^2 + m_2^2 + \cdots + m_k^2 = (k+2) m_1 m_2 \ldots m_k xy \tag{7}$$

has at most one solution (x, y) in positive integers, satisfying $x < y < m_k$.

3.2. The unicity conjecture for prime-power Markoff numbers. In this section we shall prove that the unicity conjecture is true for Markoff numbers which are powers of primes. We use the notation and the results of the previous section. The essential point is the fact that x, y, z are pairwise coprime for any solution (x, y, z) of (1), as we saw in Lemma 3.

Corollary 9. *Let $p \in \mathbb{Z}$ be an odd prime number, s be a positive integer and $m = p^s$ be Markoff number. Then the unicity conjecture is true for the number m.*

Proof. We use the same notation as in Section 3.1, $k = 1$, m is odd.

According to Lemma 3, the ideal (β) is primitive, since $\gcd(x, y) = 1$. So is the ideal $(\overline{\beta})$.

Thus, $(p) = P\overline{P}$, $P \neq \overline{P}$ for some prime ideal $P \subseteq \mathcal{R}$ is the factorization of the ideal (p) as a product of prime ideals of $\mathcal{R}$.

Therefore, we have that $(\beta)(\overline{\beta}) = (m)^2 = P^{2s}\overline{P}^{2s}$. Since both ideals (β) and $(\overline{\beta})$ are primitive and $P\overline{P} = (p)$, we have that the set $\{(\beta), (\overline{\beta})\} = \{P^{2s}, \overline{P}^{2s}\}$ is determined uniquely by the unique factorization of the ideal $(p) \subseteq \mathcal{R}$. $\square$

4. Acknowledgments. This project was carried out under the supervision of Prof. Alexandru Ghitza at the Massachusetts Institute of Technology. I am greatly indebted to my mentor for the valuable discussions and help. He taught me much algebraic number theory and directed me during the process. I want to thank Prof. Jenny Sendova for her essential comments for preparing the paper. I would like to thank to the Center for Excellence in Education and the St. St. Cyrilus and Methodius International Foundation for the opportunity to participate in this event.

REFERENCES

[1] A. Baragar. On the unicity conjecture for Markoff numbers. *Canad. Math. Bull.* **39** (1996), No 1, 3–9.

[2] G. Frobenius. Über die Markoffschen Zahlen. Berl. Ber., 1913, 458-487.

[3] A. Hurwitz. Über eine Aufgabe der unbestimmten Analyse. *Arch. der Math. u. Phys.* (3) **11** (1907), 185-196.

[4] M. G. Krein. Markoff's Diophantine equation. Appendix to *Kvant*, (1999), No 3, 35–41 (in Russian); English version: *Kvant Selecta Algebra and Analysis*, I, Math. World, **14**, AMS, Providence, RI, 1999, 121–126.

[5] A. Markoff. Sur les formes quadratiques binaires indéfinies. *Clebsch Ann.* **XVII** (1880), 379-400.

Kaloyan Slavov
"Lui Aier" Str., Bl. 115, Ap. 25
1404 Sofia, Bulgaria
e-mail: kaloyan_slavov@yahoo.com

ХИПОТЕЗАТА НА ФРОБЕНИУС ЗА УРАВНЕНИЕТО НА ХУРВИЦ

Калоян Ст. Славов

В настоящата статия доказваме хипотезата на Фробениус за числа на Марков, които са степен на нечетно просто число. Също така, формулираме съответната хипотеза за уравнението на Хурвиц и я доказваме при определени условия.