Mathematica Slovaca

Stanislav Jakubec; Karol Nemoga

On a conjecture concerning sequences of the third order

Mathematica Slovaca, Vol. 36 (1986), No. 1, 85--89

Persistent URL: http://dml.cz/dmlcz/136415

Math. Slovaca 36, 1986, No. 1, 85—89

ON A CONJECTURE CONCERNING SEQUENCES OF THE THIRD ORDER

STANISLAV JAKUBEC—KAROL NEMOGA

Introduction

At the conference on algebra applications and combinatorics (6—12 November 1983, Příhrazy, Czechoslovakia) H. Grassmann (Humboldt University, Berlin, GDR) raised the following conjecture.

Let $\{a_n\}$ be the sequence of nonnegative integers generated by the linear recurrence relation $a_{n+3}=a_{n+1}+a_n$ with initial conditions $a_0=3$, $a_1=0$, $a_2=2$. Then for $n>1$ $n \mid a_n$ iff n is prime.

It is easy to see that if n is prime, then $n \mid a_n$. (See below.) We show that the converse is not true, i.e., there is a composite number n such that $n \mid a_n$. Hence the conjecture does not hold.

As a matter of fact the authors and others have tried to disprove the statement "experimentally" by considering the sequence $\{3, 0, 2, 3, 2, 5, 5, 7, 10, \ldots\}$ up to thousand of terms.

The general considerations used in the following give the method for fast generating natural numbers for which the conjecture is not true. Moreover, such numbers are found.

I.

The characteristic equation of the sequence $\{a_n\}$ defined by $a_{n+3}=a_{n+1}+a_n$ is

$$X^3-X-1=0 \tag{1}$$

If α_1, α_2, α_3 are roots of (1) in the field of complex numbers, then with regard to the given initial conditions $a_0=3$, $a_1=0$, $a_2=2$ we have

$$a_n=\alpha_1^n+\alpha_2^n+\alpha_3^n \qquad n=0, 1, 2, \ldots$$

In the ring of algebraic integers of $Q(\alpha_1, \alpha_2, \alpha_3)$, ($Q$ is the field of rational numbers) we have

$$a_p = \alpha_1^p + \alpha_2^p + \alpha_3^p \equiv (\alpha_1 + \alpha_2 + \alpha_3)^p \equiv a_1^p = 0 \pmod{p}$$

whence $p \mid a_p$, as stated in the introduction.

Lemma 1. *Let p, q be two distinct primes. Then $a_{pq} \equiv 0 \pmod{pq}$ iff $a_p \equiv 0 \pmod{q}$ and $a_q \equiv 0 \pmod{p}$.*

Proof. We have

$$a_{pq} = \alpha_1^{pq} + \alpha_2^{pq} + \alpha_3^{pq} \equiv (\alpha_1^p + \alpha_2^p + \alpha_3^p)^q = a_p^q \pmod{q}\ .$$

By Fermat's theorem we have

$$a_p^q \equiv a_p \pmod{q}\ .$$

Hence

$$a_{pq} \equiv a_p \pmod{q} \tag{2}$$

and in the same way

$$a_{pq} \equiv a_q \pmod{p} \tag{3}$$

a) If $a_{pq} \equiv 0 \pmod{pq}$, then from (2) $0 \equiv a_{pq} \equiv a_p \pmod{q}$, which implies $q \mid a_p$. Analogously $p \mid a_q$.

b) If conversely $a_p \equiv 0 \pmod{q}$ and $a_q \equiv 0 \pmod{p}$, then by (2) and (3) $a_{pq} \equiv 0 \pmod{q}$ and $a_{pq} \equiv 0 \pmod{p}$. Hence $pq \mid a_{pq}$. This proves Lemma 1.

In the following we shall prove that it is possible to find two distinct primes p, q such that $a_p \equiv 0 \pmod{q}$ and $a_q \equiv 0 \pmod{p}$. By Lemma 1 this implies $a_{pq} \equiv 0 \pmod{pq}$.

Lemma 2. *Suppose that the polynomial $f(X) = X^3 - X - 1$ splits into linear factors over Z/pZ. Suppose moreover that the roots $\lambda_1, \lambda_2, \lambda_3$ of $f(X)$ (contained in Z/pZ) are k-th power residues modulo p and $k \mid (p-1)$. Then the period of the sequence $a_0, a_1, a_2, \ldots$ modulo p is a divisor of $(p-1)/k$.*

Proof. By supposition there are elements $\mu_i \in Z/pZ$ such that

$$\mu_i^k = \lambda_i \pmod{p} \text{ for } i = 1, 2, 3\ .$$

Put $e = (p-1)/k$. Then $\lambda_i^e = \mu_i^{p-1} \equiv 1 \pmod{p}$.

Now for any n

$$a_n = \lambda_1^n + \lambda_2^n + \lambda_3^n \equiv \lambda_1^{n+e} + \lambda_2^{n+e} + \lambda_3^{n+e} = a_{n+e} \pmod{p}\ .$$

Therefore the period of the sequence $a_0, a_1, a_2, \ldots$ modulo p is a divisor of $(p-1)/k$.

Let $K = Q(\alpha_1)$. The polynomial $f(X) = X^3 - X - 1$ is irreducible over the field Q. The discriminant of $f(X)$ is $\Delta=-23$. To be able to use Lemma 2 we have to find criteria for the factorization of $f(X)$ into linear factors modulo p.

According to [1] (Theorem 3, Chapter IV, §2) $f(X)$ splits into three different linear factors over Z/pZ for a prime $p\neq 23$ if and only if the prime p is a product of three different prime divisors in K. The conditions under which this takes place are given by the Takagi—Hasse Theorem ([2], §21). The theorem itself is as follows.

Theorem (Takagi—Hasse). *Let D_K be the discriminant of the cubic field K. The set of equivalence classes of integral binary quadratic forms with the discriminant D_K has a cardinality h, where $3\mid h$.*

One third of these classes (which can be uniquely specified) represents those primes p which are the product of three (different) prime divisors in K.

Primes representable by the remaining quadratic forms are exactly those primes p, which are prime divisors in K.

Primes which are not representable by any of the binary integral quadratic forms with discriminant D_K are exactly those primes which are the product of two different prime divisors in K. (The last case occurs iff $\left(\frac{D_K}{p}\right)=-1$.)

In our case we have the following situation.

The discriminant of the field $K=Q(\alpha_1)$ is $D_K=-23$.

The number of classes of binary integral quadratic forms with the discriminant $d=-23$ is 3. These classes are represented by the forms $X^2+XY+6Y^2$, $2X^2+XY+3Y^2$, $2X^2-XY+3Y^2$. (See, e.g., [3], p. 58, where a table of reduced quadratic forms of negative discriminant is given.)

The Takagi—Hasse Theorem implies that a prime p can be decomposed into a product of three different prime divisors in K if and only if p is representable by the quadratic form $X^2+XY+6Y^2$. Since $X^2+XY+6Y^2=((2X+Y)^2+23Y^2)/4$, the primes representable by the forms $X^2+XY+6Y^2$ and X^2+23Y^2 are the same. We have proved

Lemma 3. *The polynomial $f(X)=X^3-X-1$ splits into three different linear factors over Z/pZ ($p\neq 23$) if and only if p is representable by the quadratic form X^2+23Y^2.*

The following theorem provides sufficient conditions under which $a_{pq}\equiv 0 \pmod{pq}$.

Theorem 1. *Let p, q be primes such that*

(i) $q=1+k(p-1)$, $k>1$

(ii) *p, q are representable by quadratic form X^2+23Y^2*

(iii) *all roots of the polynomial $f(X)=X^3-X-1$ in Z/qZ are k-th power residues modulo q.*

Then $a_{pq}\equiv 0 \pmod{pq}$.

Proof. By Lemma 3 the polynomial $f(X)$ splits into three linear factors over

Z/pZ and over Z/qZ. According to Lemma 2 the period of the sequence $a_0, a_1, a_2, \ldots$ (modulo p) is a divisor of $p-1$ and the period of the sequence $a_0, a_1, a_2, \ldots$ (modulo q) is a divisor of $(q-1)/k$. Hence we have

$$a_q = a_{1+k(p-1)} \equiv a_1 = 0 \pmod{p} .$$

Since $p = 1 + (q-1)/k$ we have

$$a_p = a_{1+(q-1)/k} \equiv a_1 = 0 \pmod{q} .$$

By Lemma 1 we obtain that $a_{pq} \equiv 0 \pmod{pq}$.

II.

It remains to show that there exist couples of primes p, q which satisfy the conditions (i), (ii) and (iii) of the Theorem 1.

Example 1. Let $p = 3037 = 47^2 + 23 \cdot 6^2$ and $q = 9109 = 91^2 + 23 \cdot 6^2 = 1 + 3(3037 - 1)$.

The roots of the polynomial $f(X) = X^3 - X - 1 \pmod{9109}$ are 5193, 6391 and 6634. Since

$$\left(\frac{5193}{9109}\right)_3 = \left(\frac{6391}{9109}\right)_3 = \left(\frac{6634}{9109}\right)_3 = +1$$

Theorem 1 implies

$$a_{3037 \cdot 9109} \equiv 0 \pmod{3037 \cdot 9109} .$$

The proof of Theorem 1 does not imply that $n = 3037 \cdot 9109$ is the least positive integer n which is not prime and for which $n \mid a_n$.

Example 2. Let $p = 4831 = 68^2 + 23 \cdot 3^2$ and $q = 9661 = 47^2 + 23 \cdot 18^2 = 1 + 2(4831 - 1)$.

The roots of the polynomial $f(X) = X^3 - X - 1 \pmod{9661}$ are 854, 3342, 5465. Since

$$\left(\frac{854}{9661}\right) = \left(\frac{3342}{9661}\right) = \left(\frac{5465}{9661}\right) = +1 ,$$

the Theorem 1 implies

$$a_{4831 \cdot 9661} \equiv 0 \pmod{4831 \cdot 9661} .$$

Searching by computer (EC 1045.1 at about 20 hours of CPU time) showed that there are just five natural numbers less than $n = 3037 \cdot 9109$ (Example 1), for which the conjecture is not true. The numbers are the following $n_1 = 271\,441 = 521^2$, $n_2 = 904\,631 = 7 \cdot 13 \cdot 9941$, $n_3 = 16\,532\,714 = 2 \cdot 11^2 \cdot 53 \cdot 1289$, $n_4 = 24\,658\,561 = 19 \cdot 271 \cdot 4789$, $n_5 = 27\,422\,714 = 2 \cdot 11^2 \cdot 47 \cdot 2411$.

However, the Theorem 1 gives us a method of much faster generating counterexamples of the form $n = pq$ (computing time is more than 10^4 times shorter).

We conclude with the following remark.

The sequence $\{a_n\}$ studied above is identical with the sequence $\{s_n\}$ where s_n is the sum of the n-th powers of the roots of $X^3 - X - 1$ in Q.

The following pertinent question arises. Let $X^3 + pX + q$ be an irreducible polynomial over Q. Consider the sequence $\{s_i\}$ where s_i has the meaning just introduced. Is it true that there exists a composite integer n such that $n \mid s_n$? The answer is very probably positive.

Acknowledgement

We should like to thank professor Štefan Schwarz for his help and valueable comments.

REFERENCES

[1] БОРЕВИЧ З. И.—ШАФАРЕВИЧ И. Р.: Теория чисел. Знание. Москва 1972.

[2] ДЕЛОНЕ Б. Н.—ФАДДЕЕВ Д. К.: Теория иррациональностей третьей степени. Труды математического института имени В. А. Стеклова 11. Москва 1940. English translation: DELONE B. N.—FADDEEV D. K.: The Theory of Irrationalities of the Third Degree. AMS. Providence 1964.

[3] DICKSON L. E.: Modern Elementary Theory of Numbers. The University of Chicago Press. Chicago 1939. Second Impression 1943.

Received February 24, 1984

Matematický ústav SAV
Obrancov mieru 49
814 73 Bratislava

ОБ ОДНОЙ ГИПОТЕЗЕ, КАСАЮЩЕЙСЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ТРЕТЬЕЙ СТЕПЕНИ

Stanislav Jakubec, Karol Nemoga

Резюме

Пусть $a_0, a_1, a_2, \ldots$ обозначает последовательность целых чисел, которую определяет рекуррентное соотношение $a_{n+3} = a_{n+1} + a_n$ и начальные условия $a_0 = 3$, $a_1 = 0$, $a_2 = 2$. В статье опровергается следующая гипотеза: n простое тогда и только тогда, когда $n \mid a_n$.