Annales Mathematicae Silesianae 12 (1998), 157–160

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

PRIME PERIODS OF PERIODICAL P-ADDITIVE FUNCTIONS

STANISLAV JAKUBEC

Dedicated to the memory of Ivan Korec

I. Korec [Ko] introduced the following definition of a P–additive function.

DEFINITION. A function $F : \mathrm{N} \to \mathbf{R}$ is said to be Pythagorean-additive (P-additive, for short) if for all $x, y, z \in \mathrm{N}$

$$x^2 = y^2 + z^2 \quad \Rightarrow \quad F(x) = F(y) + F(z).$$

The aim of this paper is to determine all prime numbers that are periods of P-additive functions. The main result is the following theorem.

THEOREM. *Let the prime number p be a period of a P-additive function. Then $p \in \{2, 3, 5, 13\}$.*

PROOF. The existence of P-additive functions with the periods p in the set $\{2, 3, 5, 13\}$ is proved in [Ko].

Now we prove that there are no other periods. We start with the following theorem (see Theorem 5.6 in [Ko]).

Let $p > 5$ be a prime number and let there exist a (non-constant) periodical P-additive function with the period p. Then
(i) $p \equiv 1 \pmod 6$.

Received on October 9, 1998.
1991 *Mathematics Subject Classification.* Primary 11A25.
Key words and phrases: Pythagorean additive functions, solving congruences

(ii) *For every triple of positive integers* x, y, z *such that* p *does not divide* xyz *and* $x^2+y^2=z^2$ *there is* $j \in \{1,2,\dots,p-1\}$ *such that* $x^j \not\equiv y^j \pmod p$ *and*

$$(xy)^j \equiv z^{2j} \pmod p, \quad x^{3j}+z^{3j} \equiv 0 \pmod p.$$

(iii) *Under the assumption* (ii), *the elements* $\frac{x}{z}$ *and* $\frac{y}{z}$ *have orders divisible by* 6 *in the multiplicative group modulo* p.

This statement reduces the proof of our Theorem to the following lemma.

LEMMA. *For every prime number* $p \equiv 1 \pmod 6$, $p \neq 13$ *there exist* $x, y, z \in \mathrm{N}$ *satisfying* $x^2+y^2=z^2$, $(xyz, p)=1$ *and such that either* $\left(\frac{x}{z}\right)^j$ *or* $\left(\frac{y}{z}\right)^j$ *is not a primitive* 6*th root of unity modulo* p, *for* $j = 1, 2, \dots, p-1$.

PROOF OF THE LEMMA. Case 1. $p \equiv 3 \pmod 4$.
Put $x=3, y=4, z=5$. The number $\frac{3}{5}\cdot\frac{4}{5}=\frac{12}{25}$ is not a square in the group $(\mathrm{Z}/p\mathrm{Z})^*$, because

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Thus exactly one of the numbers $\frac{3}{5}$, $\frac{4}{5}$ is a square modulo p. If $p \equiv 3 \pmod 4$, then a primitive 6th root of 1 modulo p is a quadratic nonresidue. This proves the Lemma in Case 1.

CASE 2. $p \equiv 1 \pmod 4$ and $p \not\equiv 1 \pmod 8$.
We shall prove that for $p > 1000$ there exist (x, y, z), with $x^2+y^2=z^2$ such that $\frac{x}{z}$ is a 4th power modulo p. This fact proves Lemma in the Case 2 (after numerical examination of primes $p < 1000$) because a primitive 6th root of 1 modulo p is not a 4th power modulo p.

Let $\frac{x}{z} = \frac{2uv}{u^2+v^2}$. Put $u = x_1^4$, $v = x_2^4$, $x_1x_2 \not\equiv 0 \pmod p$, $x_1^8 - x_2^8 \not\equiv 0 \pmod p$. The number $p-1$ is not divisible by 8 and so $z = x_1^8 + x_2^8 \not\equiv 0 \pmod p$. We prove that for $p > 1000$ there exist $x_1, x_2, x_3 \in \mathrm{N}$ such that $x_1x_2 \not\equiv 0 \pmod p$, $x_1^8 - x_2^8 \not\equiv 0 \pmod p$ and

$$(*) \qquad x_1^8 + x_2^8 \equiv 2x_3^4 \pmod p.$$

Denote by N the number of solutions of (*). By Theorem 3, p. 22 in [BS] we have

$$|N - p^2| \leqslant 27(p-1)\sqrt{p}.$$

It is easy to see that the number of solutions of (*) that do not satisfy $x_1x_2 \not\equiv 0 \pmod p$, $x_1^8 - x_2^8 \not\equiv 0 \pmod p$ is at most $96p+1$. If $p > 1000$ then

$$|96p + 1 - p^2| > 27(p-1)\sqrt{p},$$

therefore there exists a solution of (*) such that $x_1x_2 \not\equiv 0 \pmod p$, $x_1^8 - x_2^8 \not\equiv 0 \pmod p$.

Let x_1, x_2, x_3 be such a solution. Then

$$\frac{x}{z} = \frac{2uv}{u^2+v^2} = \frac{2x_1^4x_2^4}{x_1^8+x_2^8} \equiv \frac{2x_1^4x_2^4}{2x_3^4} \pmod p,$$

and so $\frac{x}{z}$ is a 4th power modulo p. To complete the proof in Case 2 it is necessary to check the primes $p < 1000$ such that $p \equiv 1 \pmod 6$, $p \equiv 5 \pmod 8$, hence the primes:

$$\begin{aligned} p =& 37, 61, 109, 157, 181, 229,\\ & 541, 277, 349, 373, 397, 421, 613, 661, 709, 733, 757, 829, 853, 877, 997. \end{aligned}$$

The following list gives the values $\left(p, \frac{x}{z}\right)$ such that $\left(\frac{x}{z}\right)^j$ it is not a primitive 6th root of 1 modulo p, for $j = 1, 2, \ldots, p-1$.

$\left(p, \frac{x}{z}\right) = \left(37, \frac{5}{13}\right), \left(61, \frac{3}{5}\right), \left(109, \frac{3}{5}\right), \left(157, \frac{3}{5}\right), \left(181, \frac{3}{5}\right) \left(229, \frac{4}{5}\right), \left(277, \frac{12}{13}\right),$
$\left(349, \frac{3}{5}\right), \left(373, \frac{3}{5}\right), \left(397, \frac{3}{5}\right), \left(421, \frac{3}{5}\right), \left(541, \frac{3}{5}\right), \left(613, \frac{4}{5}\right), \left(661, \frac{3}{5}\right), \left(709, \frac{4}{5}\right),$
$\left(733, \frac{4}{5}\right), \left(757, \frac{20}{29}\right), \left(829, \frac{3}{5}\right), \left(853, \frac{3}{5}\right), \left(877, \frac{5}{13}\right), \left(997, \frac{3}{5}\right).$

CASE 3. $p \equiv 1 \pmod 8$.
Because

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1,$$

there exist $a, b \in \mathbf{Z}$ such that $a^2 \equiv -1 \pmod p$, $b^2 \equiv 2 \pmod p$. Thus

$$a^2 + b^2 \equiv 1^2 \pmod p.$$

We are now in a position to apply the following theorem proved in [Sc]:
If $\mathrm{ord}_2\, m$ *is even and there exist integers* x_0, y_0, z_0 *satisfying* $x_0^2 + y_0^2 \equiv z_0^2 \pmod m$, *then there exist integers* x, y, z *such that* $x^2 + y^2 = z^2$, $x^2 \equiv x_0^2, y^2 \equiv y_0^2, z^2 \equiv z_0^2 \pmod m$.
Using this result we conclude that there exist $x \equiv \pm a, y \equiv \pm b, z \equiv \pm 1 \pmod p$ such that $x^2 + y^2 = z^2$. Hence $\frac{x}{z} \equiv \pm a \pmod p$. Clearly $\pm a$ is a root of the polynomial $X^4 - 1 \equiv 0 \pmod p$, and so $(\pm a)^j$ is also a root of this polynomial. Hence it cannot be a primitive 6th root of 1 modulo p

because the polynomials $X^2 - X + 1$ and $X^4 - 1$ over the field $\mathbb{Z}/p\mathbb{Z}$ are relatively prime.

Now all the primes p have been verified. Thus the Lemma, and so also the Theorem, is proved. $\square$

REMARK. The referee of this paper proved that the exact number of solutions of (*) that do not satisfy $x_1x_2 \not\equiv 0 \pmod p$, $x_1^8 - x_2^8 \not\equiv 0 \pmod p$ is $16(p-1)+1$. Thus the inequality $|16p - 15 - p^2| > 27(p-1)\sqrt{p}$ holds for all primes $p > 800$ and it is sufficient to verify the primes up to 800.

REFERENCES

[BS] Z. I. Borevich and I. R. Shafarevich, *Teoriya chisel (The theory of numbers)*, Third ed., Nauka, Moscow (1985).

[Ko] I. Korec, *Additive conditions on sums of squares*, Ann. Math. Silesianae, **12** (1998), 29–43.

[Sc] A. Schinzel, *On Pythagorean triangles*, Ann. Math. Silesianae, **12** (1998), 25–27.

Matematický ústav SAV
Štefánikova 49
814-73 Bratislava
Slovakia