ON THE WEAKLY PRIME-ADDITIVE NUMBERS WITH LENGTH 4

Wing Hong Leung
Department of Mathematics, Texas A&M University, Texas
josephleung@tamu.edu

Received: 7/12/23, Accepted: 12/12/23, Published: 1/29/24

Abstract

In 1992, Erdős and Hegyvári showed that for any prime p, there exist infinitely many length 3 weakly prime-additive numbers divisible by p. In 2018, Fang and Chen showed that for any positive integer m, there exist infinitely many length 3 weakly prime-additive numbers divisible by m if and only if 8 does not divide m. Assuming the existence of a prime in certain arithmetic progressions with prescribed primitive root, which is true under the Generalized Riemann Hypothesis (GRH), we show that for any positive integer m, there exist infinitely many length 4 weakly prime-additive numbers divisible by m. We also present another related result analogous to the length 3 case shown by Fang and Chen.

1. Introduction

A number n with at least 2 distinct prime divisors is called *prime-additive* if $n = \sum_{p|n} p^{a_p}$ for some $a_p > 0$. If additionally, $p^{a_p} < n \leq p^{a_p+1}$ for all $p|n$, then n is called *strongly prime-additive.* In 1992, Erdős and Hegyvári [2] stated a few examples and conjectured that there are infinitely many strongly prime-additive numbers. However, this problem was and is still far from being solved. For example, not even the infinitude of prime-additive numbers is known. Therefore they introduced the following weaker version of prime-additive numbers.

Definition 1. A positive integer n is said to be *weakly prime-additive* if n has at least 2 distinct prime divisors, and there exists distinct prime divisors $p_1, ..., p_t$ of n and positive integers $a_1, ..., a_t$ such that $n = p_1^{a_1} + \cdots + p_t^{a_t}$. The minimal value of such t is defined to be the *length* of n, denoted as κ_n.

Note that if n is a weakly prime-additive number, then $\kappa_n \geq 3$. So we call a weakly prime-additive number with length 3 a *shortest weakly prime-additive* number.

DOI: 10.5281/zenodo.10580934

Erdős and Hegyvári [2] showed that for any prime p, there exist infinitely many weakly prime-additive numbers divisible by p. In fact, they showed that these weakly prime-additive numbers can be taken to be shortest weakly prime-additive in their proof. They also showed that the number of shortest weakly prime-additive numbers up to some integer N is at least $c(\log N)^3$ for a sufficiently small constant $c > 0$.

In 2018, Fang and Chen [3] showed that for any positive integer m, there exist infinitely many shortest weakly prime-additive numbers divisible by m if any only if 8 does not divide m. This is Theorem 5 stated in this paper. They also showed that for any positive integer m, there exist infinitely many weakly prime-additive numbers with length $\kappa_n \leq 5$ that are divisible by m. In the same paper, Fang and Chen posted four open problems. The first one inquires whether, for any positive integer m, there are infinitely many weakly prime-additive numbers n with $m|n$ and $\kappa_n = 4$. In Theorem 1 of this paper, we confirm this is true, assuming the existence of a prime in certain arithmetic progressions with prescribed primitive root (see assumption $(*)$ on p.2). This assumption is known to hold under the Generalized Riemann Hypothesis (GRH).

Finally, it was also shown in [3] that for any distinct primes p, q, there exists a prime r and infinitely many a, b, c such that $pqr|p^a + q^b + r^c$. In Theorem 2, we extend this result analogously to four distinct primes, subject to mild congruence conditions, assuming the same assumption as mentioned above.

2. Main Results

Assumption $(*)$. Let $1 \leq a \leq f$ be positive integers with $(a, f) = 1$ and $4|f$. Let g be an odd prime dividing f such that $\left(\frac{g}{a}\right) = -1$ with $\left(\frac{\cdot}{\cdot}\right)$ being the Kronecker symbol. Then there exists a prime p such that $p \equiv a \pmod{f}$ and g is a primitive root of p.

It is known that $(*)$ is a consequence of the Generalized Riemann Hypothesis (GRH), see Corollary 1 in the next section for details. Under the assumption $(*)$, we have the following.

Theorem 1. *Assume $(*)$. For any positive integer m, there exist infinitely many weakly prime-additive numbers n with $m|n$ and $\kappa_n = 4$.*

Note that if a positive integer n can be expressed in the form of $n = p^a+q^b+r^c+s^d$ for some distinct primes p, q, r, s, and positive integers a, b, c, d such that $p, q, r, s|n$, then p, q, r, s are all odd primes. We have the following theorem as a partial converse.

Theorem 2. *Assume $(*)$. For any distinct odd primes p, q, r with one of them $\equiv 3$ or $5 \pmod{8}$, there exist infinitely many prime s and infinitely many positive* *integers* a, b, c, d *such that*

$$pqrs | p^a + q^b + r^c + s^d.$$

This is analogous to Theorem 1.4 in [3], which says that for any given distinct primes p, q, there exists a prime $r > \max\{p, q\}$ and infinitely many triples (a, b, c) of positive integers such that $pqr | p^a + q^b + r^c$.

3. Preliminaries

Lemma 1 ([4, Thm 72])**.** (The Fermat-Euler Theorem) *Let* a, n *be coprime positive integers. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

where ϕ *is the Euler totient function.*

We will use the Kronecker Symbol $(\frac{\cdot}{\cdot})$, which is a generalization of the Legendre symbol. Precisely, this is defined as follows. Let a, b be integers. If $b = 0$ or $b = \pm 1$, we define

$$\left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = \pm 1 \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad \left(\frac{a}{\pm 1}\right) = \begin{cases} \pm 1 & \text{if } a < 0 \\ 1 & \text{if } a \geq 0. \end{cases}$$

For the remaining cases, let $b = \pm p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of b. We then define

$$\left(\frac{a}{b}\right) = \left(\frac{a}{\pm 1}\right) \prod_{i=1}^{k} \left(\frac{a}{p_k}\right)^{e_k},$$

where for any prime p,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

is the Legendre symbol.

Whenever we write $(\frac{a}{b})$ for some integers a, b, it refers to the Kronecker symbol. We will need the following properties of the Kroncecker symbol. See, for example, [1, p. 289-290] for a proof.

Lemma 2. *Let* a, b, c *be any nonzero integers, and* p, q *be any odd primes. Let* a', b' *be the odd part of* a *and* b*, respectively. Then we have:*

1. $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$ *unless* $c = -1$;

2. $\left(\frac{a}{b}\right) = (-1)^{\frac{a'-1}{2}\frac{b'-1}{2}}\left(\frac{b}{a}\right)$;

3. $\left(\frac{-2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1, 3 \pmod 8 \\ -1 & \textit{if } p \equiv 5, 7 \pmod 8; \end{cases}$

4. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$;

5. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *unless* $p \equiv q \equiv 3 \pmod 4$;

6. *If* $p \equiv q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

On primes in arithmetic progressions, we have the celebrated Dirichlet's theorem. See, for example, [1, Chapter 1] for a proof.

Theorem 3. (Dirichlet's Theorem) *If a, d are coprime positive integers, then there are infinitely many primes p such that $p \equiv a \pmod d$.*

Under GRH, we have the following generalization.

Theorem 4 ([5, Thm 1.3])**.** *Let $1 \le a \le f$ be positive integers with $(a, f) = 1$. Let g be an integer that is not equal to -1 or a square, and let $h \ge 1$ be the largest integer such that g is an hth power. Write $g = g_1 g_2^2$ with g_1 square free, and $g_1, g_2 \in \mathbb{Z}$. Let*

$$\beta = \frac{g_1}{(g_1, f)} \textit{ and } \gamma_1 = \begin{cases} (-1)^{\frac{\beta-1}{2}}(f, g_1) & \textit{if } \beta \textit{ is odd;} \\ 1 & \textit{otherwise.} \end{cases}$$

Let $\pi_g(x; f, a)$ be the number of primes $p \le x$ such that $p \equiv a \pmod f$ and g is a primitive root $\pmod p$. Then, assuming GRH, we have

$$\pi_g(x; f, a) = \delta(a, f, g)\frac{x}{\log x} + O_{f,g}\left(\frac{x \log\log x}{\log^2 x}\right),$$

where

$$\delta(a, f, g) = \frac{A(a, f, h)}{\phi(f)}\left(1 - \left(\frac{\gamma_1}{a}\right)\frac{\mu(|\beta|)}{\prod_{\substack{p|\beta \\ p|h}}(p-1)\prod_{\substack{p|\beta \\ p\nmid h}}(p^2-p-1)}\right)$$

if one of the following holds:

- $g_1 \equiv 1 \pmod 4$,
- $g_1 \equiv 2 \pmod 4$ *and* $8|f$
- $g_1 \equiv 3 \pmod 4$ *and* $4|f$.

Otherwise, we have

$$\delta(a,f,g)=\frac{A(a,f,h)}{\phi(f)}.$$

Here μ *is the Möbius function,* $\left(\frac{\cdot}{\cdot}\right)$ *is the Kronecker symbol, and*

$$A(a,f,h)=\prod_{p\mid(a-1,f)}\left(1-\frac{1}{p}\right)\prod_{\substack{p\nmid f\\ p\mid h}}\left(1-\frac{1}{p-1}\right)\prod_{\substack{p\nmid f\\ p\nmid h}}\left(1-\frac{1}{p(p-1)}\right)$$

if $(a-1,f,h)=1$*, and* $A(a,f,h)=0$ *otherwise.*

Corollary 1. *Assume GRH. Let* a,f,g *be as above and* $\left(\frac{g}{a}\right)=-1$*. There exists a prime* p *such that* $p\equiv a \pmod f$ *and* g *is a primitive root of* p*. In other words, assumption* $(*)$ *holds true under GRH.*

Proof. This corresponds to a special case of Theorem 4, with our specific conditions on a,f,g, $\beta=h=1$, $\gamma_1=g$. Notice that

$$\delta(a,f,g)=\frac{2}{\phi(f)}\prod_{p\mid(a-1,f)}\left(1-\frac{1}{p}\right)\prod_{p\nmid f}\left(1-\frac{1}{p(p-1)}\right)>0.$$

□

Remark 1. This shows that our result also follows from GRH, which is a much stronger assumption than $(*)$.

Theorem 5 ([3, Cor 1.1])**.** *For any positive integer* m*, there exist infinitely many shortest weakly prime-additive numbers* n *with* $m|n$ *if and only if 8 does not divide* m*.*

4. Proof of Theorem 1

We first prove the following weaker version of Theorem 1.

Theorem 6. *Assume* $(*)$*. For any positive integer* m*, there exist infinitely many weakly prime-additive numbers* n *with* $m|n$ *and* $\kappa_n\le 4$*.*

Proof. Let m be a positive integer. Write $m=2^k m_1$ with $(m_1,2)=1$ and $k\ge 0\in\mathbb{Z}$. Without loss of generality, we assume $k\ge 3$. In fact, if the theorem holds when m is replaced by $2^{\max\{3,k\}}m$, then the theorem holds for m. We will construct a family of distinct primes p,q,r,s and positive integers a,b,c such that each of m,p,q,r,s divides n, where $n:=p^a+q^b+r^c+s$.

Let p be an odd prime such that $(p, m) = 1$. By the Chinese Remainder Theorem and Theorem 3, there exists an odd prime q such that

$$q \equiv 1 \pmod{2^k p} \text{ and } q \equiv -1 \pmod{m_1}.$$

Similarly, we can use the same two theorems to conclude that there exists an odd prime r such that

$$r \equiv 3 \pmod{2^k} \text{ and } r \equiv 1 \pmod{pqm_1}.$$

Applying the Chinese Remainder Theorem again, there exists a unique integer s_0 such that $1 \leq s_0 \leq pqrm$ and

$$\begin{aligned} s_0 &\equiv -5 \pmod{2^k} \\ s_0 &\equiv -1 \pmod{m_1} \\ s_0 &\equiv -2 \pmod{pqr}. \end{aligned}$$

Note that $(s_0, pqrm) = 1$.

Since $k \geq 3$, we have $r \equiv 3 \pmod{2^k}$ and $s_0 \equiv -5 \pmod{2^k}$. This implies that $r \equiv 3 \pmod 8$ and $s_0 \equiv 3 \pmod 8$. Using Lemma 2, we observe that

$$\left(\frac{r}{s_0}\right) = \left(\frac{s_0}{r}\right)(-1)^{\frac{s_0-1}{2}\frac{r-1}{2}} = -\left(\frac{s_0}{r}\right) = -\left(\frac{-2}{r}\right) = -1.$$

Here we used $s_0 \equiv -2 \pmod r$ as $s_0 \equiv -2 \pmod{pqr}$. Therefore, applying Corollary 1 with $a = s_0$, $f = pqrm$ and $g = r$, there exists an odd prime s such that $s \equiv s_0 \pmod{pqrm}$, and r is a primitive root of s. Consequently, s satisfies all the previously mentioned congruence relations satisfied by s_0. Furthermore, there exists a positive integer c_0 such that

$$r^{c_0} \equiv -2 \pmod s.$$

Note that by construction, p, q, r, s are all distinct odd primes.

Now for any positive integer c', take

$$c = (p-1)(q-1)(r-1)\phi(m)c' + c_0.$$

For any positive odd integer b', take

$$b = \frac{1}{4}(r-1)(s-1)b'.$$

Since $r \equiv 3 \pmod{2^k}$ and $s \equiv -5 \pmod{2^k}$, we have $r, s \equiv 3 \pmod 4$, ensuring that b is odd. For any positive integer a', take

$$a = (q-1)(r-1)(s-1)\phi(m)a',$$

where ϕ is the Euler totient function. Finally, let

$$n = p^a + q^b + r^c + s.$$

Note that we have the following congruence conditions:

1. As $q \equiv r \equiv 1 \pmod{p}$, $s \equiv -2 \pmod{p}$, we have

$$n \equiv p^a + q^b + r^c + s \equiv 0 + 1 + 1 - 2 \equiv 0 \pmod{p}.$$

2. Since $q - 1|a$, Lemma 1 implies that $p^a \equiv 1 \mod q$. Hence we have

$$n \equiv p^a + q^b + r^c + s \equiv 1 + 0 + 1 - 2 \equiv 0 \pmod{q}.$$

3. Similarly, $p^a \equiv 1 \pmod{r}$ as $r - 1|a$. Since $q \equiv 1 \pmod{2^k p}$, we have $q \equiv 1 \pmod{8}$. Applying Lemma 2 with $r \equiv 3 \pmod{8}$ and $r \equiv 1 \pmod{q}$,

$$q^b \equiv (q^{\frac{1}{2}(r-1)})^{\frac{1}{2}(s-1)b'} \equiv \left(\frac{q}{r}\right)^{\frac{1}{2}(s-1)b'} \equiv \left(\frac{r}{q}\right) \equiv \left(\frac{1}{q}\right) \equiv 1 \pmod{r}.$$

So we have

$$n \equiv p^a + q^b + r^c + s \equiv 1 + 1 + 0 - 2 \equiv 0 \pmod{r}.$$

4. Similarly, $p^a \equiv q^b \equiv 1 \pmod{s}$. As $r^c \equiv -2 \pmod{s}$, we have

$$n \equiv p^a + q^b + r^c + s \equiv 1 + 1 - 2 + 0 \equiv 0 \pmod{s}.$$

5. As $\phi(m)|a$, Lemma 1 gives us $p^a \equiv 1 \pmod{m}$. Since b is odd and $q \equiv -1 \pmod{m_1}$, we get $q^b \equiv -1 \pmod{m_1}$. Together with $r \equiv 1 \pmod{m_1}$ and $s \equiv -1 \pmod{m_1}$, we have

$$n \equiv p^a + q^b + r^c + s \equiv 1 - 1 + 1 - 1 \equiv 0 \pmod{m_1}.$$

6. Since $p^a \equiv 1 \pmod{m}$, $q \equiv 1 \pmod{2^k}$, $r \equiv 3 \pmod{2^k}$ and $s \equiv -5 \pmod{2^k}$, we have

$$n \equiv p^a + q^b + r^c + s \equiv 1 + 1 + 3 - 5 \equiv 0 \pmod{2^k}.$$

As a result, $n = p^a + q^b + r^c + s$ is weakly prime additive and is divisible by m. Since a', c' can be any positive integers, b' can be any positive odd integer and p can be any arbitrary odd prime that is coprime to m, we have constructed infinitely many weakly prime-additive n with length at most 4. □

Remark 2. In the above construction, s can be raised to any d-th power for any positive integer $d \equiv 1 \pmod{\phi(pqrm)}$.

Together with Theorem 5, we can now prove Theorem 1.

Proof of Theorem 1. Let m be a positive integer. By Theorem 6, there exist infinitely many weakly prime-additive numbers with length ≤ 4 such that they are divisible by $8m$. Since $8|8m$, Theorem 5 implies that these numbers cannot be shortest weakly prime-additive, and hence they are all weakly prime-additive numbers with length 4. $\square$

5. Proof of Theorem 2

Let p, q, r be distinct odd primes, with one of them, WLOG say r, satisfying $r \equiv 3$ or $5 \pmod 8$. Let k be the positive integer such that $\frac{(p-1)(q-1)}{2^k}$ is odd. We denote this value as $A = \frac{(p-1)(q-1)}{2^k}$ and set $f = 8Apqr$. By the Chinese Remainder Theorem, there exists a unique integer s_0 such that $1 \leq s_0 \leq f$ and

$$\begin{aligned} s_0 &\equiv 3 \pmod 8 \\ s_0 &\equiv -2 \pmod{Apqr}. \end{aligned}$$

Using Lemma 2 and the condition that $r \equiv 3$ or $5 \pmod 8$, we have

$$\left(\frac{r}{s_0}\right) = (-1)^{\frac{r-1}{2}\frac{s_0-1}{2}}\left(\frac{s_0}{r}\right) = (-1)^{\frac{r-1}{2}}\left(\frac{-2}{r}\right) = -1.$$

Applying Theorem 3 with the above a, f, and $g = r$, there exists an odd prime s such that
$s \equiv s_0 \pmod{8Apqr}$ and r is a primitive root of s. In other words, r generates $(\mathbb{Z}/(s\mathbb{Z}))^*$ and hence there exists $0 < c_0 < s-1$ such that

$$r^{c_0} \equiv -2 \pmod s.$$

Since $s \equiv 3 \pmod 8$, we have $\left(\frac{-2}{s}\right) = 1$, implying that c_0 must be even.

Now by the Chinese Remainder Theorem, take any positive integer c such that

$$\begin{aligned} c &\equiv c_0 \ (\mathrm{mod}\ \frac{s-1}{2}) \\ c &\equiv 0 \pmod{(p-1)(q-1)}. \end{aligned}$$

This is feasible because $s \equiv 3 \pmod 8$ and $s \equiv -2 \pmod A$, ensuring that $(\frac{s-1}{2}, (p-1)(q-1)) = 1$. Since c_0 is even and $\frac{s-1}{2}$ is odd, this makes $c \equiv c_0 \pmod{s-1}$. Thus, we obtain $r^c \equiv -2 \pmod s$ and $r^c \equiv 1 \pmod{pq}$.

Finally, for any positive integers a, b, d such that $(q-1)(r-1)(s-1)|a$, $(p-1)(r-1)(s-1)|b$, $d \equiv 1 \pmod{(p-1)(q-1)(r-1)}$, we have the following:

$$p^a + q^b + r^c + s^d \equiv 0 + 1 + 1 - 2 \equiv 0 \pmod{p}$$
$$p^a + q^b + r^c + s^d \equiv 1 + 0 + 1 - 2 \equiv 0 \pmod{q}$$
$$p^a + q^b + r^c + s^d \equiv 1 + 1 + 0 - 2 \equiv 0 \pmod{r}$$
$$p^a + q^b + r^c + s^d \equiv 1 + 1 - 2 + 0 \equiv 0 \pmod{s}$$

Therefore, for any positive integers a, b, c, d as above, we have

$$pqrs | p^a + q^b + r^c + s^d.$$

□

References

[1] R. G. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Amer. Math. Soc., Providence, 1963.

[2] P. Erdős and N. Hegyvári, On prime-additive numbers, *Stud. Sci. Math. Hung.* **27** (1992), 207-212.

[3] J. H. Fang and Y. G. Chen, On the shortest weakly prime-additive numbers, *J. Number Theory* **182** (2018), 258-270.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford university press, Oxford, 1979.

[5] P. Moree, On primes in arithmetic progression having a prescribed primitive root. II, *Funct. Approx. Comment. Math.* **39.1** (2008), 133-144.