

# Additive structure of $Z(\cdot) \bmod [\text{prod. first } k \text{ primes}]$ , with carry extension to integer prime pair sums

NICO F. BENSCHOP - *Amspade Research*, The Netherlands

## Abstract

The product  $m_k$  of the first  $k$  primes ( $2..p_k$ ) has neighbours  $m_k \pm 1$  with all prime divisors beyond  $p_k$ , implying there are infinitely many primes [Euclid]. All primes between  $p_k$  and  $m_k$  are in the group  $G_1$  of units in semigroup  $Z_{m_k}(\cdot)$  of multiplication mod  $m_k$ . Due to its squarefree modulus  $Z_{m_k}$  is a disjoint union of  $2^k$  groups, with as many idempotents - one per divisor of  $m_k$ , which form a Boolean lattice  $BL$ . The *additive* properties of  $Z_{m_k}$  and its lattice are studied. It is shown that each complementary pair in  $BL$  adds to 1 mod  $m_k$ , and each even idempotent  $e$  in  $BL$  has successor  $e+1$  in  $G_1$ . It follows that  $G_1 + G_1 \equiv E$ , the set of even residues in  $Z_{m_k}$ , so each even residue is the sum of two roots of unity, proving "Goldbach for Residues" mod  $m_k$  ( $GR$ ). The smallest composite unit in  $G_1 \bmod m_k$  is  $p_{k+1}^2$  so its units between  $p_{k+1}$  and  $p_{k+1}^2$  are all prime, to be used as summands for successive  $2n$ . Induction on  $k$  by extending these unit residues mod  $m_k$  with 'carry'  $a < p_{k+1}$  of weight  $m_k$  yields a Euclidean prime sieve for integers. Failure of Goldbach's Conjecture ( $GC$ ) for some  $2n$  contradicts  $GR(k)$  for some  $k$ , yielding  $GC$  : Each  $2n > 4$  is the sum of two odd primes.

**Keywords:** Residue arithmetic, ring  $Z \bmod m$ , squarefree modulus,  
Boolean lattice, Euclidean prime sieve, Goldbach conjecture.

Subject msc: 11P32

## Introduction

Detailed analysis of the algebraic structure of modulo arithmetic is pursued, especially multiplication in relation to addition and exponentiation. Addition and multiplication are associative operations, so semigroup structure analysis provides a good perspective for basic problems in arithmetic [2,3,6,8] such as *Goldbach's conjecture* of every even number  $2n > 4$  being the sum of two odd primes. The additive structure of multiplicative semigroups with squarefree moduli is studied, in ring  $Z(+, \cdot) \bmod m_k$ . Choosing as modulus the product  $m_k$  of the first  $k$  primes, all primes between  $p_k$  and  $m_k$  are in the group of roots of 1 mod  $m_k$ , denoted as the group  $G_1$  of units. As shown (thm2.1),  $G_1 + G_1$  covers all even residues  $2n$  in  $Z \bmod m_k$ .

The direct product  $Z_{rs} = Z_r \times Z_s$  of multiplications with coprime component moduli  $r$  and  $s$ , is represented by component-wise multiplication [4]. Squarefree modulus  $m_k$  implies  $Z_{m_k}(\cdot) = Z_{p_1} \times \dots \times Z_{p_k}$  is a direct product of multiplications mod  $p_i$ . This direct product is analysed as an ordered *disjoint union* of maximal *subgroups* derived from the component semigroups  $Z_{p_i}$ . The emphasis is on the *additive* properties of idempotents, and the "fine structure" of residue ring  $Z(+, \cdot) \bmod m_k$ . Induction on  $k$  transfers additive results from residues to positive integers. In fact, residues  $x \bmod m_k$  are viewed as naturals  $x < m_k$  already in the earlier sections, with the natural upper bound  $x + y < 2m_k$  so a possible carry is at most 1. For instance in Lemma 1.1: the sum of each pair of complementary idempotents equals 1 mod  $m_k$ , yielding the natural sum  $m_k + 1$  for pairs other than  $\{0,1\}$ .

**Notation:** The known number representation (base  $m$ )  $n = c.m + r$  with carry  $c$  and rest  $0 \leq r < m$  is used. Operation  $+$  is natural addition, which for two summands  $< m_k$  can produce a maximal carry of 1 (base  $m_k$ ). For residue arithmetic  $c = 0$ . If no confusion can arise,  $m$  will denote modulus  $m_k$ ,  $\equiv$  denotes congruence mod  $m_k$ . Section 3 interpretes residues  $n \bmod m_k$  as naturals  $n < m_k$ , and by extension with carry  $a < p_{k+1}$  of weight  $m_k$  this yields all naturals  $n + a.m_k < m_{k+1}$ . The required proof applies induction over  $k$ .

The idempotents  $e^2 \equiv e$  of  $Z_m(\cdot)$  play an essential role. For prime modulus  $p$  it is known that  $Z_p$  has just two idempotents: 0 and 1 mod  $p$ . And all residues 1, . . . ,  $p-1$ , coprime to  $p$ , are in some permutation generated as residues of powers  $g^i$  of some *primitive root*  $g < p$  of unity [1]. They form an order  $p - 1$  cyclic subgroup  $G$  of  $Z_p$ , written  $G = g^* \equiv \{g^i\}$  ( $i = 1..p-1$ ), with  $g^{p-1} \equiv 1$ . Hence  $Z_p(\cdot)$  is a cyclic group, adjoined to zero.

**Summary:** The product  $m_k$  of the first  $k$  primes, and induction on  $k$ , are used for analysis of all primes and their additive properties. Each of the  $2^k$  divisors  $d$  of  $m_k$  yields a maximal subgroup  $G_d$  of  $Z_{m_k}$  containing all  $n < m_k$  with the same set of prime divisors as  $d$ . The respective group identities are the  $2^k$  idempotents of  $Z_{m_k}$ , ordered as Boolean lattice  $BL$  [4][6] of which the additive properties are studied.

The additive properties of  $Z_{m_k}$  are characterised by the successor  $n+1$  of any  $n$ , especially of the idempotents. An essential additive property is that each complementary pair of idempotents in  $BL$  sums to 1 mod  $m_k$  (lem1.1), and every even  $e^2 = e$  has successor  $e + 1$  in  $G_1$ , while  $G_1 + G_1$  covers all  $2n \bmod m_k$ . This residue version  $GR$  of Goldbach's Conjecture ( $GC$ ) is extended, by induction on  $k$ , to prove  $GC$  for positive integers. Results listed in the Conclusions may be new.

For completeness, these essential concepts [5][6] are reviewed in sections 1 and 2. Section 3 specifies a "Euclidean prime sieve" by induction on  $k$ , for extending residues to integers by a carry mechanism. Section 4 gives the approach to Goldbach's conjecture, followed by conclusions.

## 1 Lattice of groups

In modulus  $m_k = \prod p_i$  ( $i = 1 .. k$ ) each prime factor has exponent one. So  $m_k$ , having no square divisor, is called *square free*. The prime divisors of  $m_k$  are referred to as **base primes**.

Residues  $n$  with the same base-prime divisors as squarefree divisor  $d \mid m_k$  form a *maximal subgroup*  $G_d \subset Z_{m_k}(\cdot)$  with closure due to all possible products having the same base primes. If  $e$  is the identity (idempotent) of  $G_d$ , then each  $n$  in subgroup  $G_d \equiv G_e$  has a unique *local* inverse  $n^{-1}$  defined by  $n.n^{-1} \equiv e$ .

The  $2^k$  divisors of  $m_k$  correspond to as many subsets of the  $k$  base primes. Each divisor  $d$  of  $m_k$  generates a finite cycle  $d^* = \{d^i\}$  with an idempotent  $\underline{d}$ , the identity of subgroup  $G_d$ . Each subgroup has just one idempotent as its identity. So  $Z_{m_k}$  has  $2^k$  disjoint subgroups  $G_d$ , one for each divisor  $d$  of  $m_k$ , ordered in a Boolean lattice as their identities are ordered, as follows.

### 1.1 Ordering of commuting idempotents

$Z_{m_k}$  is a disjoint union of  $2^k$  groups  $G_d$ , and the group identities, the idempotents, form a *Boolean lattice*. In fact, *commuting idempotents*  $e^2 = e$ ,  $f^2 = f$  can be *ordered*  $e \geq f$  whenever  $ef = fe = f$ , in other words  $e$  is identity for  $f$ . This is readily verified to be an ordering relation, being transitive, anti-symmetric and reflexive [4].

The lattice *meet* (greatest lower bound) operation is modelled by *multiplication*. The product of two commuting idempotents  $e, f$  is idempotent:  $ef.ef = ef.fe = efe = eef = ef$ , while  $e, f$

are left- and right- identity for  $ef$  since  $e.ef = ef = fe = fe.e$ , so that  $e \geq ef$ , and similarly  $f \geq e$ . Also,  $ef$  is the greatest idempotent ordered under  $e$  and  $f$ , since  $c \leq e$  and  $c \leq f$  imply  $c \leq ef$ , which is easily verified.

The *join* (least upper bound) of two idempotents is the idempotent with the *intersection* of the corresponding baseprime sets. Idempotent '1' at the top has the smallest base-prime set (empty), while '0' at the bottom contains all base-primes since  $0 = m \pmod m$ .

The sum of two idempotents is generally not an idempotent, nor is its generated idempotent their lattice-join, except for complementary idempotents, to be derived next.

## 1.2 Lattice of idempotents: add vs join

As shown earlier, the set of idempotents of  $Z \pmod m$  is closed under multiplication, forming a lower semi-lattice [4,6]. *Multiplication* models the **meet** (glb: greatest lower bound) operation of two idempotents, yielding an idempotent with the *union* of the respective base-prime sets.

Notice all primes  $p : p_k < p < m_k$  are 'units' in topgroup  $G_1$ . In the base-prime set of any idempotent or subgroup they are considered equivalent to  $1 \pmod{m_k}$ . For instance, cycle  $2^* \pmod m$  (in  $G_2$ ) produces residues  $c.2^n$ , where  $c \in G_1$  are relative prime to  $m_k$ , and  $c$  has prime divisors  $p_r > p_k$ . Residues in  $G_1$  can occur as factor in each  $n \in Z_{m_k}$ , according to their name of *units* in  $Z_{m_k}$ .

The **join** (least upper bound *lub*) of two idempotents follows by *intersecting* their baseprime sets, yielding an idempotent with their common baseprimes.

**Def:** two idempotents  $a, b$  are *complementary* iff  $ab \equiv 0$  and  $\text{lub}(a, b) \equiv 1$ .

The endomorphism ' $e$ ' for idempotents  $e$  in commutative  $Z_m(\cdot)$  models the lattice meet operation by multiplication, since for each  $x, y \in Z_m : xy.e \equiv xy.e^2 \equiv xe.ye$ .

Although in general the sum of two idempotents is not an idempotent, the next exception is an essential additive property of  $Z_m(\cdot)$  :

**LEMMA 1.1** For any squarefree  $m > 1$  with at least two prime divisors:

For each complementary pair  $\{a, b\} \neq \{0, 1\}$  of idempotents in  $Z_m(\cdot)$  holds  $a + b = m + 1$ .

**PROOF.** The lattice of idempotents has order  $2^k$ , with  $2^{k-1}$  complementary pairs. Consider a sublattice of order four:  $0, 1$  and any other complementary pair  $a, b$ . It must be shown that  $a + b \equiv 1 \pmod m$ . Now idempotents  $a, b$  are complementary, so  $ab \equiv 0 \pmod m$ , implying :  $(a+b)^2 \equiv a^2 + 2ab + b^2 \equiv a + b \pmod m$ , thus  $a+b$  is idempotent. And  $(a+b)a \equiv a^2 + ba \equiv a \pmod{m_k}$ , so  $a + b \geq a$ , and similarly  $a + b \geq b$ . Hence  $a + b \equiv 1 \pmod m$ , because by  $\text{lub}(a, b) \equiv 1$  the only idempotent covering complementary  $a$  and  $b$  is 1. Clearly, for  $\{a, b\} \neq \{0, 1\}$  holds  $1 < a + b < 2m$  so  $a + b = m + 1$ , with carry =1 (base  $m$ ).  $\square$

In other words : complementary idempotents  $a, b$  have disjoint base-prime sets  $A$  and  $B$ , and union  $A \cup B$  consists of all base-primes in  $m$ . For square-free  $m$ ,  $a.b \equiv 0$  is the idempotent containing all base-primes. And  $\text{join}(a, b)$  has the trivial intersection  $A \cap B = 1$  as base-prime set, relative prime to  $m$ , with corresponding idempotent '1' of  $G_1$ .

**LEMMA 1.2** For squarefree modulus  $m = 2.\text{odd}$  :  $h = m/2$  is the lowest odd idempotent in  $Z_m(\cdot)$  and  $a \rightarrow a + h$  is the only additive automorphism of  $Z_m(\cdot)$

**PROOF.** Notice  $2h \equiv 0$ , so for each even or odd pair  $a, b$  in  $Z_m$  holds  $(a + b)h \equiv 0$ . Hence :  $(a + h)(b + h) \equiv ab + (a + b)h + h^2 \equiv ab + h$ , and only if  $h^2 \equiv h$  this yields  $a \rightarrow a + h$  as

additive automorphism of  $Z_m(\cdot)$ . Furthermore,  $h = m/2$  is the lowest odd idempotent, namely the image under  $+h$  of the lowest even idempotent 0 in  $Z_m$  (for squarefree  $m$  : no divisors of 0 exist). It is readily verified that this morphism is 1-1 onto, mapping  $Z_m(\text{even})$  and  $Z_m(\text{odd})$  into each other.  $\square$

Now consider product  $m = m_k = \prod_{i=1}^k p_i$  of the first  $k$  primes. Unit 1 is ordered at the top of the lattice of idempotents, being the identity for all idempotents in  $Z_m = \times_i Z_{p_i}$ . Top group  $G_1$  of all residues relative prime to  $m$  misses all base primes. Thus  $G_1 = \times_i C(p_i-1)$  [ $i = 2..k$ ] is a direct product of  $k - 1$  cycles of periods  $p_i - 1$ .

**COROLLARY 1.1** *In  $Z(\cdot)$  mod  $m$  with square-free  $m = 2.\text{odd}$ , and let  $h = m/2$  then:*

*Odd and even top-groups are isomorphic  $G_1 \cong G_2$  under additive automorphism  $+h$ .*

*Note: isomorphic max cycles  $(2+h)^* \cong 2^*$  in  $G_1$  and  $G_2$  (e.g.  $5 < \text{primes} < 25$  are  $15 \pm 2^i$ )*

## 2 Primes, composites and neighbours

**Equivalent sum and difference :**  $(-1)^2=1$  implies  $-1 \in G_1$ , so  $G_1 \equiv -G_1$  hence :

$$(1) \quad G_1 + G_1 \equiv G_1 - G_1$$

So sums and differences of pairs in  $G_1$  yield the same set of residues mod  $m$ . Notice that:  $(-n)^2 = n^2$ , so  $n$  and  $-n$  generate the same idempotent, thus are in the same subgroup:

$$(2) \quad \text{For every group } G_d \subset Z_m : \text{ if } n \in G_d \text{ then so is } -n, \text{ while } G_d + G_d \equiv G_d - G_d.$$

**Neighbours  $n+1$  and  $n-1$  in the lattice of  $Z_m$  :**

For integers and residues:  $n$  and  $n+1$  are coprime for each  $n$  so their prime divisors form disjoint sets. The same holds for  $n$  and  $n-1$ . Then one would expect  $n$  and  $n+1$  to be in complementary subgroups of  $Z_m$ . More precisely, the subgroup ordering of their idempotents implies:

**LEMMA 2.1** *For each  $n \in Z_m$  and base-prime complementary  $\bar{n}$  :  $G_{n\pm 1} \geq G_{\bar{n}}$*

**PROOF.** Due to the subgroup ordering, a *subset* of baseprimes disjoint from (complementary to) those in  $n$  defines a subgroup ordered above or equal to  $G_{\bar{n}}$ .  $\square$

Hence  $e+1$  for any **even** idempotent  $e$  must be in an odd subgroup  $G_d$  that is ordered  $G_d \geq G_{\bar{e}}$ , with  $\bar{e}$  the complement of  $e$  in the lattice of  $Z_m$ . In fact, as shown next:  $e+1$  is in topgroup  $G_1$ .

### 2.1 Each idempotent's successor is in $G_1$ or $G_2$

The sum of two complementary idempotents yields an idempotent namely 1 (lem1.1), which is their join or least upper bound. This is an exception, and in general idempotents do not sum to an idempotent, let alone their join. For instance, in  $Z_{10}$  with idempotents 1, 5, 6, 0 :  $5 + 1 = 6$  is idempotent, but  $\text{join}(5,1) = 1$ . And  $\text{join}(6,1) = 1$  while  $6 + 1 = 7$  is not idempotent, although 7 does generate the proper idempotent 1, due to:

**LEMMA 2.2** *In  $Z(\cdot)$  mod  $m$ , with square-free  $m = 2.\text{odd}$ :*

- (a) *Each **even** idempotent  $e$  has  $e+1$  in  $G_1$ , and*
- (b) *each **odd** idempotent  $d$  has  $d+1$  in  $G_2$ .*
- (c) *For period  $n$  of  $e + 1$  in  $G_1$  mod  $m_k$  holds:  $e.(2^n - 1) \equiv 0$ .*

PROOF. (a,c): Given  $e^2 = e$ , notice that  $(e+1)(e-1) \equiv e^2 - 1 \equiv e - 1$ , so  $e+1$  is identity for  $e-1$ , hence  $G_{e+1} \geq G_{e-1}$  for every idempotent  $e$ . Now  $(e+1)^2 \equiv e^2 + 2e + 1 \equiv 3e + 1$ , and in general expanding  $(e+1)^n$ , with  $e^i \equiv e$  for all  $i > 0$  and factoring out  $e$ , yields:

$$(e+1)^n \equiv 1 + \sum_{i=1}^n \binom{n}{i} e^i \equiv 1 + (2^n - 1)e$$

We need to show  $c = (2^n - 1)e \equiv 0$  for every even idempotent  $e$ , where  $n$  is the period of  $e+1$ , with corresponding odd idempotent  $d = (e+1)^n = c+1$ , which equals 1 iff  $c \equiv 0$ . In fact it would suffice if  $2^n - 1$  is in a group complementary to  $G_e$  in the lattice of  $Z_m$ . The baseprimes in  $2^n - 1$ , which are all necessarily odd, would then complement those in even idempotent  $e$ .

This can be seen as follows:  $d^2 = d$  implies  $(c+1)^2 \equiv c+1$ , hence  $c^2 + c \equiv 0$ , so:  $(2^n - 1)^2 e + (2^n - 1)e \equiv (2^n - 1)(2^n - 1 + 1)e \equiv (2^n - 1)2^n e \equiv 0$ .

Apparently, the odd baseprimes in  $2^n - 1$  complement at least those in  $e$  because their union is complete (product 0). This implies  $(2^n - 1)e = c \equiv 0$ , independent of the extra factor  $2^n$ . So :

**(3)**  $(e+1)^n \equiv 1 + (2^n - 1)e \equiv 1$ , where  $n$  is the period of  $e+1$  in  $G_1$ .

Part (b) is dual to (a), proven similarly by using  $G_1 \cong G_2$  (lemma 1.2)  $\square$

**THEOREM 2.1** (*Goldbach for Residues GR*):

For squarefree  $m_k = \prod p_i$  ( $i = 1 \dots k$ ) with  $p_1=2$ , and  $E$  the set of even residues mod  $m_k$ :

In  $Z \text{ mod } m_k$ :  $E \equiv \{2n\} \equiv G_1 + G_1 \equiv G_1 - G_1$ , so :

Each even residue in  $Z_{m_k}$  is a sum or difference of two units.

PROOF. In short write  $G$  for  $G_1$ . Let  $e$  be any even idempotent, then multiply  $e \in G-1$  (lem2.2) on both sides by  $G$ . On the lefthand side this yields  $G.e = G_e$  which is the max-subgroup on  $e$ , and on the righthand side  $G(G-1) = G^2 - G = G - G$ , sothat  $G_e \subseteq G - G$ . Using (1) yields:  $G_e \subseteq G - G = G + G$  for all even  $G_e$ , so  $G + G$  covers all even residues.  $\square$

This also holds for any even squarefree modulus  $m = 2 \cdot \text{odd}$ . Theorem 2.1 can be generalized for naturals by careful extension of residues with *carries*, and by induction over  $k$ , as shown next.

### 3 Euclidean prime sieve

**Define**  $G_1(k)$  as group of units mod  $m_k$ , corresponding set  $G(k)$  of naturals  $\{1, u\}$  where  $p_k < u < m_k$  and  $u$  coprime to base primes  $p \leq p_k$ , use  $G'(k)$  if excluding 1, and set  $P(k)$  of all primes in  $G(k)$ . If no confusion arises, the term *unit* is used for both residues and naturals. A *Euclidean prime sieve* with bases  $m_k$  is derived by induction on  $k$  and carry-extending  $G(k)$ .

The primes  $p > p_{k-1}$  are congruent mod  $m_{k-1}$  to units in  $G_1(k-1)$ , and all those  $p < m_k$  are covered by  $G(k-1) + a m_{k-1}$  ( $0 \leq a < p_k$ ). Notice each unit  $u \in G(k-1)$  generates at most  $p_k$  primes  $p = u + a m_{k-1} \in P(k)$ , with  $p_{k-1} < u < m_k$ . For large enough  $2n$  there are many additive prime pair representations in  $GC$  format. All units  $u$  with  $p_k < u < p_{k+1}^2$  in  $G(k)$  are prime, since  $p_{k+1}^2$  is the smallest composite in  $G(k)$ .

In fact each natural  $n < m_k$  is represented uniquely by  $k$  digits of a multi base code using the successive baseprimes:  $p_1 \dots p_k$ . The  $k-1$  lower significant digits are extended with a most significant digit or **carry**  $a < p_k$ , of weight  $m_k$ .

This in contrast to the usual single base code, e.g. decimal, using powers of ten. The successive bases 2, 6, 30, 210, ... have maximal digit values  $p_{k-1}$ : 1, 2, 4, 6, ... respectively. For instance decimal  $331 = 210 + 11^2 = 1.210 + 4.30 + 0.6 + 0.2 + 1$  yields 5-digit code 1 4 0 0 1.

**Define**  $T_a(k) \subset G(k+1)$  as the set of **extensions** of  $n \in G(k)$  by a positive digit  $a < p_{k+1}$  :

$$(4) \quad T_a(k) = G(k) + a m_k \quad \text{for } 0 < a < p_{k+1}$$

which translates  $G(k)$  by a multiple of  $m_k$ , hence  $T_a(k) \equiv G_1(k) \pmod{m_k}$  for all  $a$ .

Notice  $G(k) \cup T_a(k)$  for all  $a < p_{k+1}$  covers units set  $G(k+1)$ , thus all primes  $p > p_k$  less than  $m_{k+1}$  and their composites starting at  $(p_{k+1})^2$ . For example let  $k=3$  then  $31=1+1.30$  and smallest composite  $7^2=19+30$  in  $T_1 = G(3) + 1.30$ , while  $209 = 11.19 = 29 + 6.30 \in T_6$ .

Extensions  $T_a$  are in  $p_{k+1} - 1$  adjacent disjoint intervals of size  $m_k$  :

$$(4a) \quad G(k+1) \subset G(k) \cup \{ T_a(k) \mid 0 < a < p_{k+1} \} \quad \text{where } T_a \cap T_b = \emptyset \text{ for } a \neq b.$$

All primes  $p > 3$  are congruent to  $\{1, 5\} \pmod{6}$ , while primes  $p > p_3 = 5$  are congruent to the eight prime residues  $\{1, 7, \dots, 23, 29\} \pmod{30}$  in  $G_1(3)$ , obtained from  $G(2) = \{1, 5\}$  by  $5-1=4$  extensions with increment  $m_2 = 6$ , namely  $\{7, 11\}$  ;  $\{13, 17\}$  ;  $\{19, 23\}$  ;  $\{25, 29\}$ .

Composite  $25 = 5^2$  is not coprime to 30, hence is not in  $G(3)$ . The other seven extensions are all primes  $p_3 < p < 30 = m_3$ , forming with 1 the units in  $G_1(3) = C_2 \times C_4$ , in fact of form  $15 \pm 2^i$  (cor1.1). The  $7-1=6$  extensions  $T_a(3)$  of  $G(3)$  generate all  $2.4.6 = 48$  units in  $G(4)$  : the 5 composites  $11.\{11, 13, 17, 19\}$  and  $13^2$ , and all  $6.8 - 5 = 43$  primes in open interval  $(7, 210)$ .

### 3.1 Pair sums of carry extended units

**Def:** set  $S_0(k) = G(k) + G(k)$  of pair sums of units, if excluding 1:  $S_0'(k) = G'(k) + G'(k)$ , and denote even numbers set  $E(k) = \{4 < 2n < 2m_k\}$ .

Table 1 shows these sums for  $k=2$  and 3 (by commutation half an array suffices).

Notice  $G(2) = \{1, 5\}$  with pair sums  $S_0(2) = \{2, 6, 10\}$  and pair sums  $2n$  in  $S_0'(3) = G'(3) + G'(3)$  where  $G'(3) = \{7, \dots, 29\}$  coprime to  $2.3.5 = 30 = m_3$ , with  $2p_4 \leq 2n < 2m_3$ , in interval  $[14, 58]$ . Moreover  $S_0(2) + m_2 = \{8, 12, 16\}$  and  $S_0(2) + 9m_2 = \{56, 60, 64\}$  are required to extend  $S_0(2) \cup S_0'(3)$  to cover  $E(3)$ , using 3 and 5 to avoid non-prime 1.

In fact all  $2n > 20$  have several  $GC$  pair sums, e.g. each  $2n$  in  $S_0(2) + 6c = \{2, 6, 10\} + 6c$  for  $c > 2$  has distinct unit pair sums many of which are prime pair sums.

### 3.2 Induction base: pair sums of primes in $G(3)$

**Def:** the set  $P_c(k)$  of primes in extension  $T_c = G(k) + c m_{k-1} \subset G(k+1)$ . Then by (4) :

$$(4b) \quad P_a(k) + P_b(k) \subseteq G(k) + G(k) \pmod{m_k} \quad \text{for } a, b \geq 0.$$

So the cover mod  $m_k$  given by prime sums over  $P(k)$  is **not** extended in the induction step to prime pair sums over  $P(k+1)$ . Essential is that if some  $2n < m_k$  would have no  $GC$  pair sum, this would contradict  $GR(k)$  [thm2.1], not to be covered by residues for larger  $k$ .

**Def:** set  $S_{a+b}(k) = T_a(k) + T_b(k) = S_0(k) + (a+b)m_k$  is the set of pair sums of extended units, with carries  $0 \leq a, b < p_{k+1}$ .

For instance extend  $m_2=6$  to  $m_3=30$  ( $p_3 = 5$ ) then translations  $S_{a+b}$  of  $S_0=\{2,6,10\}$  yield  $2(5-1) = 8$  diagonals of  $2 \times 2$  sums with carries  $a+b < 2(p_3-1)$  (table 1) :

$$S_1\{8, 12, 16\} \quad S_2\{14, 18, 22\} \quad S_3\{20, 24, 28\} \quad S_4\{26, 30, 34\}, \dots, S_8\{50, 54, 58\}$$

Use pair sums over  $\{3,5\}$  to avoid non-prime 1 for representing even numbers  $6, 8, 10 < 2m_2 = 12$ .

**Def:** Set  $E(k)$  of all even numbers  $2n$  with  $4 < 2n < 2m_k$ , where  $E(3)$  is induction base to cover  $E_k$  ( $k > 3$ ) by pair sums of odd primes  $p < m_k$ . (re: the Goldbach conjecture, to be proven by induction on  $k$ )

Extending  $G(2) = \{1, 5\}$  yields  $G(3) = \{G(2) + 6a \mid 0 < a < 5\}$ , containing prime set  $P(3) = \{15 \pm 2^i, 29\} < m_3$  ( $i=1,2,3$ ) where  $5^2$  is not coprime to 30, so not in  $G(3)$ .

LEMMA 3.1 (induction base  $k=3$ ): Let  $P''(3) = P(3) \cup \{3, 5, 31, 37\}$  then :

$$P(3) = G(3), \text{ and } P''(3) + P''(3) \text{ covers } E(3).$$

PROOF. By complete inspection: Increments 4 in  $S_0(2) = \{2, 6, 10\}$  cause successive  $S_c$  with carry increment 6 to *interlace*, but only for induction base  $k=3$ . Next sum range  $S_0'(3) = G'(3) + G'(3) = \{14, 18, 20, \dots, 52, 54, 58\}$  has  $incr=2$  except at both ends  $\{14, 18\}$  and  $\{54, 58\}$ .

This *edge effect* is solved by including primes  $5 \in G(2)$  and  $31, 37 \in G(4)$  with adjacent  $k \pm 1$ , corresponding to edge carry sums  $c$  of 1 and  $9 = 2p_3 - 1$ . They yield missing prime sums  $16=5+11$ ,  $44=13+31=7+37$ ,  $50=19+31=13+37$  and  $56=19+37$ , while  $7 \in G(3)$  with  $\{3, 5\}$  provides 6,8,10,12. Hence  $E(3) = \{2n \in [6, 60]\}$  is covered by pair sums of primes  $p < m_3$  in  $G(3)$ , extended with neighbouring primes 3, 5 and 31, 37.  $\square$

| Ta+Tb          | 0                       | 1                    | 2          | 3     | 4     | : carry b (wgt 6) |
|----------------|-------------------------|----------------------|------------|-------|-------|-------------------|
| -----#_1_5 #   | 7_11                    | 13_17                | 19_23      | 25_29 | 31_35 | : translations Tb |
| 1   .2. 6      | <- 6= 3+3               |                      |            | xx    |       | xx                |
| 0 5   6 .10.   | <- S0(2) = {2,6,10}     |                      |            |       |       |                   |
| #-----#<-----  | S0'(3) ----->#          |                      |            |       |       |                   |
| 7   8 12       | .14. 18                 |                      |            |       |       |                   |
| 1 11   12 >16< | 18 .22.                 |                      |            |       |       |                   |
| a Ta           | +-----*                 |                      |            |       |       |                   |
| 13   14 18     | 20 24   .26. 30         | <- S4(2) = S0(2)+4.6 |            |       |       |                   |
| 2 17   18 22   | 24 28   30 .34.         | <- = {26,30,34}      |            |       |       |                   |
|                | +-----*-----+           |                      |            |       |       |                   |
| 19   20 24     | 26 30   32 36           | .38. 42              |            |       |       |                   |
| 3 23   24 28   | 30 34   36 40           | 42 .46.              |            |       |       |                   |
|                | +-----*-----+ . . . . . |                      |            |       |       |                   |
| 5.5 x 26       | 30   32 36              | 38 42 >44<           | 48 >50<    | 54 x  |       |                   |
| 4 29   30 34   | 36 40                   | 42 46 48             | 52 54 .58. |       |       |                   |
| -----*         | #<-----                 |                      |            |       |       | #-----            |
| -> 31   32 36  | 38 42 <44>              | 48 <50>              | 54 >56<    | 60    |       |                   |
| 5 5.7 x 36     | 40 42 46                | 48 52 54             | 58 60 64   | x     |       |                   |
|                | +-----*-----+           |                      |            |       |       |                   |
| -> 37   38 42  | 44 48 <50>              | 54 <56>              | 60 62 66   |       |       |                   |

**Table 1** Extension sums: carry sum diagonal  $a + b = c$  covers  $\{2n, 2n \pm 4\} = S_0(2) + 6c$

So pair sum set  $S_0''(3)$ , adapted for the interlacing edge-effect, covers adjacent  $2n$  in  $E(3)$ . Hence interlacing does not occur for  $k > 3$ , and a unique carry sum  $a + b = c$  suffices for covering successive  $2n$  by unit pair sums, in adjacent and disjoint extension sum intervals  $S_c(k)$ , while:

(5) Each  $2n$  in  $E(k + 1)$  has a unique carry sum  $c$  with  $0 \leq c \leq 2(p_k - 1)$ , and  $2n \in S_c(k)$ .

This is to be used as induction base for  $k > 3$ , first for unit pair sum sets  $S_c(k)$ .

**Def:** The set  $S_0(k) = G(k) + G(k)$  of pair sums of units is called *complete* if it covers  $E(k)$ , otherwise it is *incomplete*.

LEMMA 3.2 (induction step for unit pair sums) Using  $S_0''(3)$  for  $S_0(3)$ , then for  $k \geq 3$  :

Extension sums  $S_c(k)$  for  $0 \leq c \leq 2(p_{k+1} - 1)$  partition  $E(k + 1)$  iff  $S_0(k)$  covers  $E(k)$ .

PROOF. Extension pair sumsets  $S_c(k)$  are disjoint and cover  $E(k+1)$  only if  $S_0(k) \supseteq E(k)$ , seen as follows. By (4) the  $T_a(k)$  are disjoint, and if  $x$  and  $y$  are in distinct extensions  $T_a(k)$  and  $T_b(k)$ , then so are their extensions under any shift  $s = c.m_k : x \neq y \leftrightarrow x + s \neq y + s$ . For distinct carrysums  $c < c'$  with  $c' - c = d : S_c(k) \cap S_{c'}(k) = S_c(k) \cap (S_c(k) + d.m_{k-1}) = \emptyset$ . Their union covers  $E(k)$  only if pair sums  $S_0(k) = G(k) + G(k)$  cover  $E(k)$ . Because some  $2n$  missing from  $S_0(k)$  implies its translations  $2n' = 2n + c.m_k$  are also missing from all  $S_c(k)$  for  $c > 0$ .  $\square$

### 3.3 Excluding composites in $G(k)$ , baseprimes and 1 as summands

In the described extension pair sum procedure, diagonals with *constant carry difference*  $a - b = d$  are parallel to main diagonal  $a = b$  ( $d=0$ ), see (4a) and table 1. Only diagonals with  $d \geq 0$  suffice because addition is commutative. The two sets of diagonals, of constant sum resp. difference, form an orthogonal coordinate pair that is relevant to prime sum analysis, with a unique extension carrysum  $c$  for each  $2n$  as essential property (5).

The regular diagonal pattern is broken by removing composites. After re-indexing, the remaining primes grow faster than linear with their index, due to the gaps left by composites. One might expect this to cause some  $2n$  to disappear from  $P(k) + P(k)$ . But such failure of  $GC$  would contradict thm2.1 ( $GR$ ), to be shown in the next section. First are discussed some details on composites in  $G(k)$ , non-prime 1, and avoiding base primes as summands except for some small  $2n$  in the induction base  $E(3) < 2.30$ .

Units group  $G(k)$ , coprime to baseprimes  $2 \dots p_k$ , contains  $p_{k+1}$  as smallest prime, so the smallest composite in  $G(k)$  is  $(p_{k+1})^2$ . Notice  $G(3)$  has no composites since  $(p_4)^2 = 49 > 30 = m_3$ . Furthermore, the units  $u \in G(4)$  are in interval  $(7 < u < 210)$  with smallest prime  $p_5 = 11$ , hence minimal composite  $11^2 = 121$ , so all units of  $G(4)$  in  $[11, 11^2)$  (coprime to  $2.3.5.7=210$ ) are prime. By inspection all  $2n$  in interval  $[22 \dots 222]$  are covered by prime pair sums, of which those  $2n < 210$  involve no carry.

The known Bertrand's Postulate is useful (Chebyshev 1850, simplified by S.Pillai 1944) to prove a complete cover of even naturals:

**BP** (*Bertrand's Postulate*): For each  $n > 1$  there is at least one prime between  $n$  and  $2n$ .

Notice that Pillai's proof [7] has an induction base of  $2n \leq 60$  (see present section 3.2). In order to guarantee prime summands, consider only pair sums of units  $u < (p_{k+1})^2$ , the smallest composite in  $G(k)$ . Successive  $k$  yield  $2n$  in overlapping intervals by  $BP$ , thus covering all  $2n$  beyond the induction base. Using  $p_{k+1} < 2p_k$  (by Bertrands Postulate) the next lemma is readily verified, regarding the absence of a carry for  $k > 4$ .

**LEMMA 3.3** For  $k \geq 5$  all prime pairsums  $2n$  with condition  $2p_{k+1} \leq 2n < 2(p_{k+1})^2$  have upperbound  $2(p_{k+1})^2 < m_k$  (starting at  $k = 5$  with  $p_{k+1} = 13$  and  $2(p_6)^2 = 338 < 2310 = m_5$ ), so no carry is produced in such prime pair sums.

Notice that for initial  $G_1(2) = \{1, 5\} \pmod{6}$  (table 1) the baseprimes 2 and 3 are not used in pair sum residues  $G_1(2) + G_1(2) = \{2, 6, 10\}$ . Considering  $2n > 4$  (re Goldbach's conjecture): non-prime 1 is avoided by  $6 = 3 + 3$  and  $8 = 5 + 3$ , the only  $2n$  requiring 3. Moreover,  $12=5+7$  and  $16=5+11$  are the only extension pair sums  $< 60$  with one summand of carry=0 (lem3.1), thus requiring baseprime 5 of  $G(3)$ .

**COROLLARY 3.1** For  $k > 3$  :

Each  $2n > p_k$  in  $E(k)$  is in an extension sum  $S_c(k-1)$  with carrysum  $0 < c \leq 2(p_k - 1)$ , having  $c > 0$  pair sums over extensions  $T_a(k-1)$  of  $G(k-1)$ , with carries  $0 < a < p_k$ .

## 4 Proving $GC$ via $GR(k)$ by induction on $k$

”Goldbach for residues” ( $GR$  thm2.1) resulted from structure analysis of arithmetic mod  $m_k$ . With  $E = \{2n\}$  and primeset  $P$  it seems that  $GR: G_1 + G_1 = E \pmod{m_k}$ , for all  $k$ , is weaker than  $GC: P + P = E$ , since  $GR$  includes composites and holds only for residues. Clearly  $GC$  implies  $GR$ , since  $P + P = E$  for integers implies equivalence for any modulus, while  $P \subseteq G_1$ .

**Approach :**  $GR \rightarrow GC$  is equivalent to  $not(GC) \rightarrow not(GR)$ . Prove  $GC$  for integers by contradiction to  $GR$ , extending residue arithmetic mod  $m_{k-1}$  with carry  $a < p_k$  as in the Euclidean prime sieve (4). If  $GC$  would fail for some  $2n > 2p_k$  then a contradiction to  $GR$  mod  $m_k$  is derived for some  $k$ .

**THEOREM 4.1** (*Goldbach’s prime pair sums*) *Each  $2n > 4$  is a sum of two odd primes.*

**PROOF.** Use Euclidean primesieve (4) with prime summands  $p_{k+1} \leq p < (p_{k+1})^2$  in units  $G(k)$ , and apply induction over  $k$ . For  $k=3$  the primes in  $P''(3) = P(3) \cup \{3, 5, 31, 37\}$  are used, with  $P''(3) + P''(3)$  covering all  $4 < 2n < 60$  (lem3.1). If  $k = 4$  the theorem holds by inspection for all  $2n$  in interval  $[22, 210 = m_4]$ , hence no carry is produced in each prime pair sum.

Each induction step for  $k > 4$  restricts summands to units  $p \in G(k)$  in half open interval  $[p_{k+1}, (p_{k+1})^2)$ . So these units are all prime, denoted by primeset  $P'(k)$ . By lemma 3.3 no carry is produced in prime pair sums  $2n$  from  $2p_{k+1}$  to  $2(p_{k+1})^2$ . Furthermore, Bertrands Postulate  $BP$  implies overlapping intervals for successive  $k$ , covering all  $2n$  beyond the induction base.

Now assume  $GC$  to fail for some  $2n$  in interval  $(2p_{k+1}, [p_{k+1}]^2)$ , thus excluding composite summands while the Bertrand Postulate guarentees overlapping intervals. Then  $S_0(k)$  is *incomplete* (lemma 3.2), along with all extensions  $S_0(k) + c.m_k$ , yielding *incomplete*  $S_0(k+1)$ . By prime sieve structure (4) with  $G_1(k+1) \equiv G_1(k) \pmod{m_k}$  based on carry extension, the missing  $2n$  would not be covered by pair sums mod  $m_i$  ( $i > k$ ) either. But this contradicts theorem 2.1 ( $GR$ ), establishing Goldbach’s Conjecture ( $GC$ ).  $\square$

Regarding the values of prime summands that suffice to cover all even naturals, the following can be said. Notice that in table 1 (for  $2n < 60$ ) only primes  $p \geq p_k$  are required to represent  $2n \geq 2p_k$  in most cases. However, exeptions occur if prime gap  $p_{k+1} - p_k > 2$ . Then  $2n + 2$  requires a prime  $p_{k-1}$  or smaller: the larger the gap the smaller  $p_{k-i}$  is required. See for instance (table 1):  $2n = 2p_k + 2 = 16, 28, 40$  for  $p_k = 7, 13, 19$  respectively, which require  $p_{k-1}$  as Goldbach summand, due to a gap  $p_{k+1} - p_k = 4$  (versus gap 2 in cases  $p_k = 5, 11, 17$ ).

## 5 Conclusions

Balanced analysis of multiplication and addition in relation to each other, with finite square-free moduli  $2...p_k$  yields a fruitful analysis of prime sums (Goldbach), similar to that with prime power moduli mod  $p^k$  for  $p$ -th power sums (Fermat [3], Waring [8]). In both approaches the careful extension of residues with a carry is essential for transferring additive structural results to integers. This ’residue-and-carry’ method, as used for proving FLT [3] and Goldbach’s Conjecture, is based on unique number representation by residue and carry: using the associative (semigroup) properties of the residue closure combined with an induction proof by carry extension. As such it could well serve as a generic method to solve other hard problems in elementary number theory [6].

In fact, the semigroup  $Z_m(.)$  of multiplication mod  $m$  is formed by the *endomorphisms* of the additive cyclic group  $Z_m(+)$  generated by 1. So  $Z_m(.) = endo[ Z_m(+)]$  where  $(.)$  distributes

over (+), suggesting a strong link between these two operations, evident from the derived additive fine structure of  $Z_{m_k}$  for squarefree modulus  $m_k$ . A two-dimensional table of prime pair sums revealed additive properties of  $2n < 2m_3 = 60$  as induction base, hard to find otherwise.

The product  $m_k$  of the first  $k$  primes as modulus restricts all primes between  $p_k$  and  $m_k$  to the group  $G_1$  of units. The additive structure of  $Z(\cdot) \bmod m_k$  was analysed, and extended to positive integers by induction on  $k$ , starting with  $k=3$  ( $Z_{30}$ ). Units group  $G_1$ , and the additive properties of the Boolean lattice  $BL$  of idempotents of  $Z_{m_k}(\cdot)$  play an essential role.

The lower semilattice of  $BL$  is multiplicative, since the *meet*  $\text{glb}(a, b)$  of two idempotents is their product. The additive properties of  $BL$  were analysed, regarding the *join*  $\text{lub}(a, b)$  in the upper semilattice. Although  $BL$  is not closed under (+) mod  $m_k$ , this yields the next main results :

Lem1.1: Each complementary pair of idempotents in  $Z_{m_k}(\cdot)$  sums to 1 mod  $m_k$

Cor1.1: Congruent max cycles  $2^* \cong (2+h)^*$  in  $G_2 \cong G_1$ , with  $h^2 \equiv h = m_k/2$

Lem2.2: Each even [odd] idempotent  $e^2 \equiv e$  has  $e+1$  in  $G_1$  [in  $G_2$ ]

Thm2.1: Each residue  $2n \bmod m_k$  is a sum of two units : *Goldbach for Residues*  $GR_k$

Sect3: Euclidean prime sieve: unit sums  $G_1(k) + G_1(k) \bmod m_k \longrightarrow$  prime sums  $P'(k) + P'(k)$

Goldbach Conjecture  $GC$  holds by induction of  $GR(k)$  over  $k$ , since failing  $GC$  contradicts  $GR$ .

## References

1. T.Apostol: "Introduction to Analytical Number Theory" thm 10.4-6, Springer Verlag '76.
2. N.Benschop: "The semigroup of multiplication mod  $p^k$ , an extension of Fermat's Small Theorem, and its additive structure", *Semigroups and Applications* p7, Prague, July'96.
3. N.Benschop: "Additive structure of the Group of units mod  $p^k$ , with Core and Carry concepts for extension to integers", Acta Mathematica Univ. Bratislava (nov.2005)  
[http://pc2.iam.fmph.uniba.sk/amuc/\\_vol74n2.html](http://pc2.iam.fmph.uniba.sk/amuc/_vol74n2.html) (pp169-184, incl. direct FLT proof)
4. G.Birhoff, T.Bartee: "Modern Applied Algebra", McGraw-Hill, 1970.
5. A.Clifford, G.Preston: "The Algebraic Theory of Semigroups", Vol.I, AMS survey #7, p130-135, 1961.
6. S.Schwarz: "The Role of Semigroups in the Elementary Theory of Numbers", *Math.Slovaca* V31, N4, pp369-395, 1981.
7. K.Chandrasekharan: "Introduction to Analytic Number Theory" (Ch.7 - Thm 4), Springer Verlag, 1968.
8. N.Benschop: "Powersums representing residues mod  $p^k$ , from Fermat to Waring", *Computers and Mathematics, with Applications*, V39 (2000) N7-8 pp253-261.