

Additive structure of $Z(\cdot) \bmod m_k$ (squarefree), and Goldbach's Conjecture

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

Abstract The product m_k of the first k primes ($2 \cdot p_k$) 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 $G_1(k)$ 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 $G_1(k) + G_1(k) \equiv E(k)$, 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). Complete inspection shows that GC holds for $k=3$. For $k > 3$ all (principle values of) units between p_k and the smallest composite $[p_{k+1}]^2$ are prime, with pairwise carry-free addition. With Bertrand's Postulate $p_{k+1} < 2 \cdot p_k$ this establishes GC .

Keywords: Semigroup, Residue arithmetic, Carry-free addition, ring $Z \bmod m$,
Square-free modulus, Boolean lattice, Goldbach's Conjecture.

Subject msc: 11P32

1 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 (thm 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 analyzed 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 $Z(+, \cdot) \bmod m_k$. Considering the principle values of units in units group $G_1(k)$ transfers additive results from residues to positive integers. So residues $u \bmod m_k$ are taken as naturals $u < m_k$, with upper bound $u + v < 2m_k$ so a possible carry is at most 1, and for sum $u + v < m_k$ no carry is produced. For instance in Lemma 1: the sum of each pair of complementary idempotents equals 1 mod m_k , yielding the natural sum $m_k + 1$ for pairs $\neq [0, 1]$.

Notation: The known number representation (base m) $n = c \cdot m + r$ with carry c and residue $0 \leq r < m$ is used. Operation $+$ is natural addition, which for two summands $< m$ produces a maximal carry of 1 (base m). For residue arithmetic apply reset $c = 0$, yielding a *subsemigroup* of the integers under addition $Z(+)$, respectively of $Z(\cdot)$. This in contrast to the usual interpretation of a residue arithmetic closure as an *image* semigroup Z/Z_m of the integers Z , consisting of residue classes to express irrelevance of the carry in residue arithmetic (mod m).

In short, these additive and multiplicative interpretations, with residue values vs. residue classes, correspond to $n = r + 0.m$ resp. $n = r + Z.m$, resetting the carry to 0 or to set Z . The latter interpretation is a mix of numbers and sets, which is cumbersome and not required in the present additive analysis. Furthermore, m will denote modulus m_k if no confusion can arise, and \equiv denotes congruence mod m_k . Section 3 interprets residues $n \bmod m_k$ as naturals $n < m_k$ by taking their principle value, restricting $2n$ to $2p_k < 2n < [p_{k+1}]^2 < m_k$ for $k > 3$ to guarantee primepair sums with carry-free addition.

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 is 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 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 characterized 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 (lemma 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 considering the set of principle values (naturals) $G(k)$ of the units in $G_1(k)$ for $k \geq 3$, to prove GC for positive integers. The Conclusion results may be new.

For completeness, these essential concepts [5][6] are reviewed in sections 1 and 2. Section 3 derives a 'Goldbach-for-Residues'(GR) result. Sections 4 and 5 give the approach to Goldbach's conjecture, followed by conclusions.

2 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 called **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, as follows.

2.1 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 $ef = fe = f$, hence 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 modeled by *multiplication*. The product of two commuting idempotents e, f is idempotent: $ef.ef = effe = efe = eef = ef$, while e, f are left- and right- identity for ef since $e.ef = ef = fe = fe.e$, so that $e \geq ef$, and similarly $f \geq ef$. 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 $0 = m \bmod m$.

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.

2.2 Lattice of idempotents: add vs join

As shown earlier, the set of idempotents of $Z \bmod m$ 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 that 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 $1 \bmod m_k$. For instance, cycle $2^* \bmod m$ (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 $lub(a, b) \equiv 1$.

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 For idempotents in $Z_m(\cdot)$ (squarefree m with at least two prime divisors): each complementary pair $\{a, b\} \neq \{0, 1\}$ has $a + b = m + 1$.

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 $a + b \equiv 1 \bmod m$. Now idempotents a, b are complementary, so $ab \equiv 0 \bmod m$, implying : $(a+b)^2 \equiv a^2 + 2ab + b^2 \equiv a + b \pmod{m}$, thus $a + b$ is idempotent. And $(a+b)a \equiv a^2 + ba \equiv a \bmod m_k$, so $a + b \geq a$, and similarly $a + b \geq b$. Hence $a + b \equiv 1 \bmod m$, because by $lub(a, b) \equiv 1$ 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 $join(a, b)$ has the trivial intersection $A \cap B = 1$ as base-prime set, relative prime to m , with corresponding idempotent '1' of G_1 .

Lemma 2 For squarefree modulus $m = 2 \cdot \text{odd}$: $h = m/2$ 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 that $2h \equiv 0$, 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 *In $Z(\cdot)$ mod m with square-free $m = 2.\text{odd}$, and $h = m/2$ then: Odd and even topgroups are isomorphic $G_1 \cong G_2$ with 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 ± 2^i)*

3 Primes, composites and neighbours

Equivalent sum or difference : $(-1)^2 = 1 \Rightarrow -1 \in G_1$ so $G_1 \equiv -G_1$ and:

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

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:

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

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

Proof. By subgroup ordering, a *subset* of base-primes disjoint from those in n defines a subgroup ordered above or equal to $G_{\bar{n}}$. \square

Hence $e+1$ for any **even** idempotent e is 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 top-group G_1 .

3.1 Each idempotent's successor is in G_1 or G_2

The sum of two complementary idempotents yields an idempotent namely 1 (lemma 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 4 *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 :

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

Part (b) is dual to (a), proven similarly by using $G_1 \cong G_2$ (cor. 1) \square

Theorem 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 $e \in G - 1$ (lem 4) 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 $G(G-1) = G^2 - G = G - G$, so that $G_e \subseteq G - G$. By (1): $G_e \subseteq G - G = G + G$ for all even G_e , so $G + G$ covers all even residues. \square

This also holds for any even squarefree modulus $m = 2.\text{odd}$. Theorem 1 can be generalized to hold for naturals which are the principle values of the units in groups $G_1(k)$, as shown next.

4 Prime units and carry extension

Define $G_1(k)$ as group of units mod m_k , and the corresponding set $G(k)$ of principle values (naturals) $\{1, u\}$ where $p_k < u < m_k$ with u coprime to base primes $p \leq p_k$. Use set $P(k)$ of all primes in $G(k)$. The emphasis is on the principle (natural) values in $G(k)$ of units in $G_1(k)$.

The primes $p > p_k$ are congruent mod m_k to units in $G_1(k)$, and all those $p < m_{k+1}$ in $G_1(k+1)$ are covered by $G(k) + a m_k$ (carry $a : 0 \leq a < p_{k+1}$). An example for $k=3$ with all units in $G_1(4)$ follows (table 1). It illustrates the relation between the prime structures of $G_1(k)$ and $G_1(k+1)$, which is a generalization of the known fact that all primes $p > 3$ are congruent to $G_1(2) = \{1, 5\}$ mod $m_2=6$: remove the numbers that have a base prime as divider (re Eratosthenes' prime sieve). Here : $G_1(4) \cong G_1(3) \text{ mod } m_3=30$.

The set of all units in $G_1(k+1)$ is generated as illustrated for $G_1(4)$ in table 1, including all primes in $P(k+1)$. Each natural unit $u \in G(k)$ generates at most $p_{k+1} - 1$ primes $p = u + a.m_k \in P(k+1)$, with $p_k < p < m_{k+1}$ and carry $0 \leq a < p_{k+1}$. Apart from 1, p_{k+1} is the smallest natural unit in $G(k)$, so $(p_{k+1})^2$ is its smallest composite, hence:

Lemma 4a: All principle values u of units in $G_1(k)$, with $p_{k+1} \leq u < (p_{k+1})^2$, are prime.

Units:	1	7<	11	13	17	19	23	29 :	mod m3 = 30
+30:	31	37	41	43	47	7^2<	53	59	p_{k+1} = 7
+60:	61	67	71	73	7.11<	79	83	89	7.n (8x '<')
+90:	7.13<	97	101	103	107	109	113	7.17<	not in G(4) (baseprime 7)
+120:	11^2#	127	131	7.19<	137	139	11.13#	149	Composites # Smallest 11^2 in G(4)
+150:	151	157	7.23<	163	167	13^2#	173	179	
+180:	181	11.17#	191	193	197	199	7.29<	11.19#	mod m4= 210

Table 1 Unit extensions: $G(k+1) = \{u + a.m_k\}$, unit $u \in G(k)$, carry $a < p_{k+1}$

Moreover, principle values of composite units in $G_1(k)$ are necessarily generated under multiplication by the corresponding prime principle values $> p_k$ of units in $G_1(k)$. The reverse process of unit reduction by multiples of m_k yields the next lemma:

Lemma 5 Let $G_1(k+1) \rightarrow G_1(k) \pmod{m_k}$ symbolize that group $G_1(k)$ is an epimorphic image of $G_1(k+1)$. The morphism is additive: $v = t + c.m_k$, relating each principle value $t \in G_1(k)$ to p_{k+1} principle values $v \in G_1(k+1)$ with a carry c .

Proof. The mappings $v - c.m_k \rightarrow t$ form a morphism: $v.w \equiv (t + c.m_k)(u + d.m_k) \equiv (t.u) + e.m_k \equiv t.u \pmod{m_k}$, where $e = (td + cu) + cd.m_k$. \square

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.

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 $p_3-1=5-1=4$ extensions with increment $m_2 = 6$, hence $\{7, 11\}$; $\{13, 17\}$; $\{19, 23\}$; $\{25, 29\}$.

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 8 units in $G_1(3) = C_2 \times C_4$, in fact of form 15 ± 2^i (cor 1). The $7-1=6$ extensions $G(3) + a.m_3$ generate all $2.4.6 = 48$ units in $G_1(4)$: the 5 composites with prime divisors $p > 7$ (exclude eight non-units of form $7.n$ in table 1), identity 1 and all $48 - 6 = 42$ primes in open interval $(7, 210)$.

4.1 Pair sums of carry extended units

Define set $S_0(k) = G(k) + G(k)$ of pair sums of (natural) units.

Denote even numbers interval by set $E(k) = \{2n \mid 4 < 2n < m_k\}$, and the set of natural carry-extended units: $T_a(k) = G(k) + a.m_k$ ($a < p_{k+1}$) in $G(k+1)$. The set of baseprimes is extended by p_{k+1} , so its multiples in $G(k+1)$ are not units (see table 1 for expanding $G(3)$ to $G(4)$ by baseprime 7). All other extended units of $G(k)$ are units of $G(k+1)$: none is divisible by a baseprime $p \leq p_{k+1}$.

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

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

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

Lemma 7 For $k \geq 3$:

Extended pairsum sets $S_c(k)$ for $0 \leq c < p_k$ partition $E(k+1) \iff S_0(k)$ covers $E(k)$.

Proof. Extension sets $S_c(k) = S_0(k) + c.m_k$ are disjoint for different carries $c < p_{k+1}$, and $\{x, y\}$ in distinct extension sum sets remain so under any shift $s = c.m_k$: $x \neq y \iff x + s \neq y + s$. 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 $S_c(k)$ with $c > 0$. \square

4.3 Proof of GC via GR and carry-free addition of prime units

The set $G(k)$ of principle values (naturals) of units in group $G_1(k)$ 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 that $G(3)$ has no composites since $(p_4)^2 = 49 > 30 = m_3$. Furthermore, the natural 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 lemma 6). In order to guarantee prime summands, consider only pair sums of units $u < (p_{k+1})^2$, the smallest composite in $G(k)$. In fact using $p_{k+1} < 2p_k$ by Bertrands Postulate (BP), the smaller interval $p_k < u < 2(p_{k+1})$ already suffices. Successive k yield $2n$ in overlapping intervals by *BP*, thus covering all $2n$ beyond the induction base $k=3$. And for $k > 3$ follows:

Lemma 8 For (natural) units in $G(k)$ and prime pairsums $2n$ with $2 p_{k+1} \leq 2n < (p_{k+1})^2$ holds: no carry is produced for $k \geq 4$ since sum upperbound $(p_{k+1})^2 < m_k$ $[(p_{4+1})^2 = 121 < m_4 = 210]$.

Notice that for initial $G(2) = \{1, 5\} \pmod 6$ (table 2) the baseprimes 2 and 3 are not used in pair sum residues $G(2) + G(2) = \{2, 6, 10\}$. 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 < 30 with one summand of carry=0, requiring baseprime 5 of $G(3)$.

Approach to GC : Consider $G(k)$ (sect. 4) as set of 'natural units' $< m_k$ congruent to the units in group $G_1(k)$ of residues mod m_k , as defined in the previous section. In other words, consider only the *principle values* of the residue units in $G_1(k)$. Let $2n$ be small enough, namely $2 p_{k+1} \leq 2n < (p_{k+1})^2$ with necessarily only prime unit summands. Then the 5-step proof of GC is as follows:

Theorem 2 (*Goldbach's Conjecture*):

Each $2n > 4$ is a sum of two odd primes.

Proof. Using $GR(k)$ (theorem 1) and carry-free addition (lemma 8):

1. For $k = 3$: GC holds by complete inspection (lemma 6).
2. For $k > 3$, as summands use the principle values $u \in G(k)$ of the units in $G_1(k)$, restricted to $p_k < u < (p_{k+1})^2$, which by lemma 4a are all prime.
3. For $k > 3$ primepair sums $2n < (p_{k+1})^2$ in $G(k) + G(k)$ yield carry=0 (lemma 8).
4. Such restricted intervals of $2n$ for successive k intersect (by Bertrand's Postulate).
5. The union over $k \geq 3$ of such primepair sums $2n$ in $G(k) + G(k)$ yield GC , because failure for some $2n$ would contradict $GR(k)$ (thm.1) for some k .
In fact by lemma 7: incomplete $S_0(k)$ [$k > 3$] implies incomplete $S_0(k - 1)$, and by repeated reduction follows incomplete $S_0(3)$, contradicting lemma 6. \square

Regarding the values of prime summands that suffice to cover all even naturals, the following can be said. Notice that in table 2 (for $2n < 30$) only primes $p \geq p_k$ are required to represent $2n \geq 2p_k$ in most cases. However, exceptions 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 2): $2n = 2p_k + 2 = 16, 28, 40$ 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 $2 \dots p_k$ 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 $Z_m(\cdot)$ of multiplication mod m is formed by the *endomorphisms* of the additive cyclic group $Z_m(+)$ generated by 1. So $Z_m(\cdot) = \text{endo}[Z_m(+)]$ where (\cdot) 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 $2n < m_3 = 30$ as basis for the analysis, 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 $Z(\cdot) \text{ mod } m_k$ was analyzed, and extended to positive integers by considering the principle values (naturals) of residues, starting with $k=3$ (Z_{30}). Units group $G_1(k)$, 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 analyzed, 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 :

Lem 1: Any complementary pair of idempotents in $Z_{m_k}(\cdot)$ sums to 1 mod m_k

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

Lem 4: Each even [odd] idempotent $e^2 \equiv e$ has $e+1$ in G_1 [in G_2]

Thm 1: *Goldbach for Residues* $GR(k)$:

Each residue $2n \bmod m_k$ is a sum of two units.

Consider principle value set $G(k)$ of units mod m_k in group $G_1(k)$.

Lem 4a: Restrict $2n \in G(k) + G(k)$ to prime sums $2p_{k+1} \leq 2n < (p_{k+1})^2$.

Lem 5: Epimorphism $G_1(k+1) \rightarrow G_1(k) \bmod m_k$.

Thm 2: Goldbach Conjecture GC holds, via a proof by finite reduction:

incomplete $S_0(k+1) \rightarrow$ *incomplete* $S_0(k)$ and contradiction to complete $S_0(3)$.

References

1. T.Apostol: "*Introduction to Analytical Number Theory*" thm 10.4-6, Springer 1976.
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" (incl. direct FLT proof), *Acta Mathematica Univ. Bratislava* (nov.2005)
http://pc2.iam.fmph.uniba.sk/amuc/_vol74n2.html (pp169-184)
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.

Author: dr. Nico F. Benschop

Drossaardstraat 71, 5663GJ Geldrop, The Netherlands

email: nfbenschop@onsbrabantnet.nl