A FINITE ANALOGUE OF THE GOLDBACH PROBLEM

ECKFORD COHEN

1. Introduction. In this paper we consider the problem of expressing the elements of the ring $R_m$ of residue classes modulo an integer $m > 1$ by sums of prime elements of $R_m$. It is convenient to assume the ring $R_m$ to be represented by integers of a complete residue system (mod $m$). Suppose $m$ has the factorization

\[ m = q_1^\mu_1 \cdots q_r^\mu_r, \]

as a product of powers of distinct primes $q_1, \ldots, q_r$. Then every element $n$ of $R_m$ may be represented in the form

\[ n = q_1^{c_1} \cdots q_r^{c_r} \xi, \quad (\xi, m) = 1, \]

where $0 \leq c_i \leq \mu_i$ ($i = 1, \ldots, r$), and the $c_i$ are uniquely determined (Lemma 3).

We say an element $\eta$ is a unit in $R_m$ if $(\eta, m) = 1$. Two elements $\alpha, \beta$ of $R_m$ are said to be associated if $\alpha = \beta \eta$ where $\eta$ is a unit. On the basis of the above representation, the primes of $R_m$ are simply the elements associated with the (ordinary) primes dividing $m$. Thus an element (1.2) is a prime of $R_m$ if and only if it is of the form $n = q_i \xi$ [4, p. 294]. In case $m$ is even, we may classify the elements $n$ of $R_m$ into even or odd according as 2 does or does not appear in the factorization (1.2) of $n$.

The basic problems arising in the additive arithmetic of primes in $R_m$ are the following: (1) For what integers $m$ does there exist a number $G(m)$ such that every element of $R_m$ is expressible as a sum of $G(m)$ primes of $R_m$? For those $m$ for which $G(m)$ exists, what is the minimum value $g$ of $G(m)$? (2) For a given $m$, determine $H(m)$, if it exists, such that every element of $R_m$ is expressible as a sum of at most $H(m)$ primes in $R_m$.

The answers to these questions are given in the following two theorems:

**Theorem 1.** There exists a number $G(m)$ such that every element of $R_m$ is expressible as a sum of $G(m)$ primes in $R_m$ if and only if $m$ has at least two distinct prime factors. For such $m$, the minimum value $g$ of $G(m)$
is given by \( g = 2 \) if \( m \) is odd, by \( g = 3 \) if \( m \) is even and has at least two distinct odd prime factors or if \( m \) is twice an odd prime power, and by \( g = 4 \) if \( m \) is of the form \( m = 2^\mu p^\lambda \) where \( \lambda \geq 1, \mu > 1 \), and \( p \) is an odd prime.

**Theorem 2.** Every number of \( R_m \) is expressible as a sum of at most three primes in \( R_m \) if and only if \( m \) has at least two distinct prime factors. Every number of \( R_m \) is a sum of at most two primes in \( R_m \) if and only if \( m \) is odd with at least two distinct prime factors or \( m \) is even and is of the form \( m = 2^\mu p, \mu \geq 1, p \) an odd prime.

These results are proved in \( \S 3 \) where several related theorems are also stated. \( \S 2 \) is concerned with lemmas required in the proofs of the above theorems. The reader is reminded of the double significance attached in this paper to the term "prime," which is used in connection with both ordinary integers and elements of \( R_m \). The distinction between the two uses, however, will be clear by the context.

2. Preliminary lemmas and remarks. We mention first the following result [1, Theorem 6]: If \( q \) is a prime and \( a_1, \ldots, a_t \) are integers prime to \( q \), \( t \geq 1 \), and \( a_{t+1}, \ldots, a_s \) (\( s \geq t \)) are integers divisible by \( q \), then the number of representations \( v(n) \) of an integer \( n \) in the form

\[
(2.1) \quad n \equiv a_1 x_1 + \cdots + a_s x_s \pmod{q^\mu}
\]

(\( \mu > 0 \)) in \( x_j \) prime to \( q \) is given by

\[
(2.2) \quad v(n) = q^{1-q^{-1}+t} (q-1)^{s-t} \left\{ (q-1)^t + (-1)^t J(n) \right\},
\]

where \( J(n) = q - 1 \) or \( -1 \) according as \( q \mid n \) or \( q \notmid n \).

From this theorem we deduce the following result basic to this paper.

**Lemma 1.** Under the conditions of the above theorem, (2.1) is insolvable in \( x_j \) prime to \( q \) if and only if one of the following cases holds:

(a) \( q \) odd, \( t = 1, q \mid n \),

(b) \( q = 2, t \) odd, \( n \) even,

(c) \( q = 2, t \) even, \( n \) odd.

We next state

**Lemma 2.** If \( b_1, \ldots, b_s \) are arbitrary integers, then

\[
(2.4) \quad n \equiv b_1 x_1 + \cdots + b_s x_s \pmod{m}
\]

is solvable in \( x_j \) prime to \( m \) if and only if each of the congruences,
has a solution in $x_j$ prime to $q_i(1.2)$.

This is a special case of the following more general result: Let $N(n, m)$ and $N(n, q_i^{\mu_i})$ represent the number of solutions, of the prescribed type, of (2.4) and (2.5) respectively. Then

$$N(n, m) = N(n, q_1^{\mu_1}) \cdots N(n, q_r^{\mu_r}).$$

**Lemma 3.** Every element $n$ of $R_m$ is representable in the form (1.2); this representation is unique except for the unit multiple $\xi$.

**Proof.** Every element of $R_m$ can be expressed in the form $n = q_1^{a_1} \cdots q_r^{a_r}$, $(\tau, m) = 1$, where $e_i \geq 0$. By Lemma 2, each of the congruences

$$q_i^{\mu_i} y_i \equiv q_i^{\mu_{i+1}} \pmod{m}$$

has a solution $y_i$ prime to $m$. Therefore the above representation of $n$ can be reduced to the form (1.2). If there were two such representations (1.2) of $n$, differing in more than the unit multiple $\xi$, we would have

$$n = q_1^{e_1} \cdots q_r^{e_r} \equiv q_1^{d_1} \cdots q_r^{d_r} \eta \pmod{m},$$

where $(\xi, m) = (\eta, m) = 1$; $\mu_i \geq c_i$, $d_i \geq 0$; and for some $i$, $c_i \neq d_i$. Supposing $i = 1, \mu_i \geq c_i > d_i$, (2.7) would imply that $q_2^{d_2} \cdots q_r^{d_r} \eta \equiv 0 \pmod{q_1}$, a contradiction.

For a detailed study of the rings $R_m$ and related rings, see Fraenkel [2] and Vandiver [4]. For a more general discussion of the ideal theory of commutative rings we mention the work of E. Noether [3]. Since the primes of $R_m$ are simply the generators of the prime ideals of $R_m$, one may view the uniqueness of the representation (1.2) as a special case and illustration of Noether's multiplicative ideal theory relative to the ring $R_m$. We note that Lemma 3 is also a special case of a result proved in [2, Lemma 2].

We make two remarks about congruences, relevant to §3:

**Remark 1.** A number $n \in R_m$ is a sum of $s$ primes in $R_m$ if and only if the congruence $n = \alpha_1 x_1 + \cdots + \alpha_s x_s \pmod{m}$ is solvable in integers $x_j$ prime to $m$ and in $\alpha_j$ (ordinary) primes dividing $m$; or what is the same, if and only if there exist ordinary primes $\alpha_1, \cdots, \alpha_s$ dividing $m$, such that each of the congruences $n = \alpha_1 x_1 + \cdots + \alpha_s x_s \pmod{q_i^{\mu_i}}$ ($i = 1, \cdots, r$) is solvable in $x_j$ prime to $q_i$.

**Remark 2.** If $q$ is a prime, then the congruence $qk \equiv qx_1 + \cdots + qx_s \pmod{q^{\lambda}}$, $\lambda \geq 1$, is solvable in $x_j$ prime to $q$ if and only if the congruence $k \equiv x_1 + \cdots + x_s \pmod{q^{\lambda-1}}$ has such a solution.
The first remark follows from Lemma 2 while the second is obvious.

3. Proofs of the theorems. We first refer briefly to terminology and notation. A congruence will be termed *solvable* if it has a solution whose coordinates are all prime to the modulus; similarly, a congruence will be termed *insolvable* if no such solution exists. In view of the necessity of distinguishing between the prime 2 and odd primes in the factorization of \(m\) (Lemma 1), the notation used in the representation (1.1) of \(m\) will be discarded in this section. Instead, odd primes dividing \(m\) will be denoted by \(p_i\); the exponents \(\mu, \lambda\) appearing in the factorization of \(m\) will be assumed positive. Finally, we shall assume in the proofs that \(n\) is represented in the form described in Lemma 3.

A. Proof of Theorem 1. In the first place, if \(m\) is the power of a prime, then no unit can be represented as a sum of primes in \(R_m\). Hence \(G(m)\) does not exist in this case. We may therefore suppose in the following that \(m\) has at least two distinct prime factors.

Suppose now that \(m\) is odd, \(m=p_1^{\mu_1} \cdots p_h^{\mu_h} \ (h \geq 2)\). If \((n, m) = 1\), then the congruence \(n \equiv p_1x_1 + p_2x_2 \pmod{m}\) is solvable by Lemmas 1 and 2. Thus on the basis of Remark 1, every such \(n\) is a sum of two primes in \(R_m\). In case \(n\) is a nonunit of \(R_m\), then it may be assumed to have a prime factor, say \(p_1\), in common with \(m\). For such \(n\), by Lemma 1, the congruence \(n \equiv p_1x_1 + p_1x_2 \pmod{p_1^{\nu_1}}\) is solvable \((\nu_1 > 1)\). Further, it is solvable \((\pmod{p_1^{\nu_1}})\) by Remark 2 and Lemma 1. Thus we see that all nonunits are sums of two primes of \(R_m\).

If \(m\) is assumed to be even, \(m = 2^{\nu}p_1^{\lambda_1} \cdots p_h^{\lambda_h} \ (h \geq 1)\), then not every element of \(R_m\) is expressible as a sum of two primes in \(R_m\). Such an element is \(r = p_1^{\lambda_1} \cdots p_h^{\lambda_h}\). For let us consider

\[
\tau = \pi_1x_1 + \pi_2x_2,
\]

where \(\pi_1\) and \(\pi_2\) are assumed to be prime divisors of \(m\). By Lemma 1, in order that (3.1) be solvable \((\pmod{2^\nu})\), one coefficient \(\pi\) must have the value 2 while the other must be odd \((\pi_1 = p_1, \pi_2 = 2, \text{say})\). But in this case (3.1) is insolvable \((\pmod{p_1^{\nu_1}})\). The assertion regarding \(r\) follows then by Remark 1.

If \(m\) is even and of the form \(m = 2^{\nu}p_1^{\lambda_1} \ (\lambda_1 \geq 2)\), then three primes will not suffice. In this case we consider

\[
4p_1 = \pi_1x_1 + \pi_2x_2 + \pi_3x_3,
\]

where the \(\pi_i\) have for value either 2 or \(p_1\). For this congruence to be solvable \((\pmod{2^\nu})\), one must have by (2.5) essentially one of two cases: (1) \(\pi_1 = \pi_2 = \pi_3 = 2\), or (2) \(\pi_1 = \pi_2 = p_1, \pi_3 = 2\). But in the first case, (3.2) cannot be solvable \((\pmod{2^\nu})\) by Remark 2 and Lemma 1,
while in the second case, (3.2) is insolvable (mod $p_1^{\mu_1}$). Thus $4p_1$ is not a sum of three primes in $R_m$. On the other hand, four primes will suffice in this case. First, if $n$ is odd, then the congruence $n \equiv p_1 x_1 + 2x_2 + 2x_3 + 2x_4 \pmod{m}$ is solvable, using Lemmas 1 and 2. Similarly if $n$ is even, the congruence $n \equiv p_1 x_1 + p_1 x_2 + 2x_3 + 2x_4 \pmod{m}$ is solvable. Hence, application of Remark 1 shows that every element $n$ is a sum of four primes of $R_m (m = 2^{\mu_1} p_1^{\mu_1}, \mu \geq 2)$.

Now consider the remaining cases, $m = 2^{\mu_1} p_1^{\mu_1}$ or $m = 2^{\mu_1} p_1^{\mu_1} \cdots p_h^{\mu_h} (h \geq 2)$. If $n$ is odd, then the congruence $n \equiv p_1 x_1 + 2x_2 + 2x_3 (\pmod{m})$ is solvable, in both cases, by Lemmas 1 and 2. If now $n$ is even, consider

\[ n \equiv 2x_1 + 2x_2 + 2x_3 \quad (n = 2k, \ k \ \text{odd}), \]

\[ n \equiv p_1 x_1 + p_2 x_2 + 2x_3. \]  

As in the previous argument, (3.3) is solvable (mod $2^{\mu_1} p_1^{\mu_1}$) and (3.4) is solvable (mod $2^{\mu_1} p_1^{\mu_1} \cdots p_h^{\mu_h}$). Thus for both cases of $m$, every element of $R_m$ is expressible as a sum of three primes in $R_m$. This completes the proof of Theorem 1.

B. Proof of Theorem 2. To prove Theorem 2 it suffices to show that if $m = 2^{\mu_1} p_1^{\mu_1} (\mu \geq 2)$, then every element of $R_m$ is a sum of two or three primes in $R_m$, and that in case $m = 2^{\mu_1} p_1^{\mu_1} (\mu \geq 1)$, any element of $R_m$ is a prime or a sum of two primes in $R_m$. It is clear that two primes will not suffice if $m$ is even and not of the form $2^{\mu_1} p_1^{\mu_1} (\mu \geq 1)$, because in such a case the element $\tau$ (3.1) is neither a prime nor a sum of two primes in $R_m$.

First we suppose $m = 2^{\mu_1} p_1^{\mu_1} (\mu \geq 1)$. If $n$ is even, $n \equiv 0 \pmod{4}$, then (3.3) is solvable (mod $m$). In case $n \equiv 0 \pmod{4}$, the congruence $n \equiv 2x_1 + 2x_2 \pmod{m}$ is solvable, while if $n$ is odd, $n \equiv p_1 x_1 + 2x_2 + 2x_3$ is solvable (mod $m$). The arguments are similar to the preceding. Applying Remark 1, it follows then that all elements of $R_m$ are sums of at most three primes in $R_m$.

Now suppose $m = 2^{\mu_1} p_1$. If $(n, m) = 1$, then the congruence $n \equiv p_1 x_1 + 2x_2 \pmod{m}$ is solvable. If $n \equiv 0 \pmod{4}$, in which case $\mu$ may be supposed $>1$ by the representation of Lemma 3, then it follows as above that $n \equiv 2x_1 + 2x_2 \pmod{m}$ is solvable. Further, if $n \equiv 0 \pmod{2p_1}$, then the congruence $n \equiv p_1 x_1 + p_1 x_2$ is solvable (mod $m$). In all other cases, $n$ is a prime of $R_m$. It thus follows that every non-prime of $R_m$ is a sum of two primes in $R_m$.

C. We now state some other theorems, all of which can be proved by the method used in the preceding proofs.
Theorem 3. If \( m \) is even, then every even element of \( R_m \), with the possible exception of the primes associated with 2, is expressible as a sum of two primes in \( R_m \).

Theorem 4. If \( m \) is even, then 2 and its associates are not sums of two primes in \( R_m \) if and only if \( m \equiv 0 \pmod{4} \) and \( m \) has at most one distinct odd prime divisor.

Theorem 5. If \( m = 2^a p_1^{\lambda_1} \cdots p_n^{\lambda_n} (n \geq 1) \), then an odd number \( n \) of \( R_m \) is not expressible as a sum of two primes of \( R_m \) if and only if \( n \) is divisible by every odd prime dividing \( m \).

Theorem 6. If \( m = 2^a p_1^{\lambda_1} (n \geq 2) \), then a number \( n \) of \( R_m \) cannot be represented as a sum of three primes of \( R_m \) if and only if \( n \) is of the form \( 2^a p_1^b \xi \) where \( a \geq 2 \), \( b \geq 1 \), and \( (\xi, m) = 1 \).

References


Institute for Advanced Study