On Composite Moduli from the Viewpoint of Idempotent Numbers

Thesis

Joseph Vass

vass31@yahoo.com

Eötvös Loránd University
Budapest, Hungary
2004

Contents

1 Introduction **2**

2 Basic Definitions **4**

3 Idempotent Numbers **5**

4 Normal Numbers **8**

5 Regular Numbers **10**

6 Binomial Congruences **24**

7 Generalized Primitive Roots **27**

8 Number Theoretic Functions **29**

9 Idempotent Numbers as an Algebraic Structure **34**

10 Second-Degree Polynomials **38**

1 Introduction

The purpose of this paper is to introduce basic concepts, as of yet unknown, that are fundamental in the examination of composite moduli, while avoiding the notoriously difficult problem of prime-factorization. We introduce a new class of numbers, called the set of idempotent numbers, that is unavoidable when researching composite moduli. Among many interesting results, we give generalizations of well-known theorems and definitions, such as the Euler-Fermat Theorem and the concept of primitive roots. We consider the generalization of the equivalence condition for the solvability of a binomial congruence to be the main result of our paper.

The paper is organized into sections of definitions, theorems, and notes. We intended to include every single result known to us regarding idempotent numbers, so as to propagate any further research that may be done on the subject by other authors. We provide basically no references, since we were unable to find any, on this particular part of Number Theory. Some of the simpler results however, may be known to group theorists, or may be found among exercises in textbooks. Since we publish all of our results, it is no surprise that the reader may find incomplete lines of thought within the network of theorems. We welcome and surely appreciate any helpful comments and papers that would be related to them.

Many of our notes in this paper are meant to provide insight to the reader into our aims of research currently in progress. As we have formerly mentioned, the paper itself is concerned with revealing all the known implications of the existence of a set, called the set of idempotent numbers, modulo a composite number.

In the next section, we provide definitions and notations, which will be used throughout the paper.

In the section "Idempotent Numbers", we give results which show the fundamentality of this set, whenever we wish to explore the hazy structure of composite moduli. We also give a generalization of the definition of order, based on our generalization of the well-known Euler-Fermat Theorem.

In the section "Normal Numbers", we define a set, which has quite a hazy structure, although not as much as the whole of $\mathbb{Z}_m$.

In the section "Regular Numbers", we introduce the nicest and most general set, that one can work with, when examining composite moduli. We are going to show many properties for this set, that have only been known so far for its subset of reduced residues, and we will also partition it into subsets of Abelian groups. We also give several other definitions and results, to the best of our knowledge, as of yet unknown.

The next section is the most important one, since it contains the main result of this paper, which is an equivalence condition for the solvability of a binomial congruence, to the greatest degree of generality, we could hope to reach. This condition is currently difficult to calculate in practice.

The next section generalizes the well-known definition of primitive roots to composite moduli. It includes only a few results, which implies that it needs the most intensive level of research, since we believe that revealing the structure of generalized primitive roots, shall also solve the problem of calculating the condition we have spoken of above.

The section "Number Theoretic Functions", introduces functions defined through definitions of previous sections, all of them containing the idea of idempotent numbers.

The set of idempotent numbers shows interesting algebraic properties, as revealed in the next section. Some nice operators may be defined over its elements, which are analogous

to operators known from Set Theory. We will also show that idempotent numbers form a commutative ring.
Our last section, entitled "Second-Degree Polynomials", discusses their sets of solutions, and in some special cases, characterizes them as well, with the use of idempotent numbers.

2 Basic Definitions

Let $\mathbb{N}$ denote the set of whole numbers greater than or equal to 1. By "number" we will mean any whole number. In the entire paper, let m denote a fixed integer, and let

$$m = \prod_{i=1}^{\infty} p_i^{\alpha_i}, \ p_i \ prime, \ p_i < p_{i+1}, \ \alpha_i \in \mathbb{N} \cup \{0\}, \ i \in \mathbb{N}$$

be the prime-factorization of m.
m is said to be square-free if $\alpha_i \leq 1$ for all $i \in \mathbb{N}$.

$$\omega(m) := |\{i \in \mathbb{N} : \alpha_i > 0\}|$$

We shall call m a weakly even number, if $p_1 = 2$ and $0 \leq \alpha_1 \leq 2$.
Furthermore, we shall call m a barely even number, if $p_1 = 2$ and $\alpha_1 = 1$.
Let $\Rightarrow$ denote logical inference. Let "iff" mean logical equivalence, or "if and only if", and let it be denoted by $\Leftrightarrow$. Let $\exists$ denote existence ($\exists!$ meaning "exists exactly one"), and $\forall$ the logical term "for all".

$$\mathbb{Z}_m := \{1, \ldots, m\}$$

In case of $A \subset \mathbb{Z}_m, \ a \in \mathbb{Z}$

$$a \in_m A \Leftrightarrow \exists b \in A : a \equiv b \pmod{m}$$

Let a mod m denote the number $b \in \mathbb{Z}_m$ for which $a \equiv b \pmod{m}$.
In case of $A \subset \mathbb{Z}$

$$A \bmod m := \{a \bmod m : \ a \in A\}$$

Let (a, b) denote the greatest common divisor of the numbers a and b.
Also, in case of $A \subset \mathbb{N}$, let $\gcd(a : a \in A)$ denote the greatest common divisor of all the elements in A.
Let $[a, b]$ denote the least common multiple of the numbers a and b.
Also, in case of $A \subset \mathbb{N}$, let $\mathrm{lcm}(a : a \in A)$ denote the least common multiple of all the elements in A. In case of an integral vector $a \in \mathbb{N}^n, \ n \in \mathbb{N}$, let $[a]$ denote the least common multiple of the coordinates of a.
Let $\varphi(m)$ denote the number of integers relatively prime to, and not exceeding m.
Furthermore, let $\psi(m)$ denote

$$\psi(m) := \mathrm{lcm}(\varphi(p_i^{\alpha_i}) : \ \alpha_i > 0)$$

(Note that if m is weakly even, then the maximal order modulo m is $\psi(m)$.)
For $a, b \in \mathbb{Z}$, let $a \mid b$ denote that a is a divisor of b.
In case of vectors $a, b \in \mathbb{Z}^n, \ n \in \mathbb{N}$, and any relation $\sim$, let $a \sim b$ mean that $a_i \sim b_i$ for all $1 \leq i \leq n$.
Let $Dom(f)$ denote the domain of function f.
Regarding other basic notations and theorems on congruences, see [1].

3 Idempotent Numbers

Definition 3.1 *A number e is said to be idempotent modulo m, if*

$$e^2 \equiv e \pmod{m}$$

Let E_m denote the subset of idempotent numbers in $\mathbb{Z}_m$.

We will mostly denote an idempotent number by e. The notation comes from the first letter of the Hungarian word for "unit", since there may be defined groups in $\mathbb{Z}_m$, with their units being idempotent numbers modulo m.
If m has only one prime factor, then $\mathrm{E}_m = \{1, m\}$.

Theorem 3.1 *For all $a \in \mathbb{Z}$*

$$a^{\varphi(m)} \in_m \mathrm{E}_m$$

Proof Let $i \in \mathbb{N}$ be a fixed number, and $\alpha_i > 0$. There are two possibilities.
1. $p_i \mid a$
Since

$$\alpha_i = 1 + (\alpha_i - 1) \leq 2^{\alpha_i - 1} \leq p_i^{\alpha_i - 1} \leq p_i^{\alpha_i - 1}(p_i - 1) \leq \varphi(m)$$

we have

$$a^{\varphi(m)} \equiv 0 \pmod{p_i^{\alpha_i}}$$

2. $p_i \nmid a$
In this case, by the Euler-Fermat Theorem (and $\varphi(p_i^{\alpha_i}) \mid \varphi(m)$), we have

$$a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$$

In both cases 1. and 2., we have

$$a^{\varphi(m)}(a^{\varphi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}}$$

so for all $i \in \mathbb{N}$ we have

$$(a^{\varphi(m)})^2 \equiv a^{\varphi(m)} \pmod{p_i^{\alpha_i}}$$

which means that

$$(a^{\varphi(m)})^2 \equiv a^{\varphi(m)} \pmod{m}$$

so $a^{\varphi(m)}$ is idempotent modulo m. □

Theorem 3.2 *For all $a \in \mathbb{Z}$*

$$a^{\psi(m)} \in_m \mathrm{E}_m$$

Proof The proof goes the same way as above, by changing each $\varphi(m)$ to $\psi(m)$. □

Many interesting facts follow from the two theorems above. One is that every polynomial is equivalent to a polynomial of degree less than or equal to $2\psi(m) - 1$ (modulo m).

Theorem 3.3 *For all $a \in \mathbb{Z}$*

$$a^{\varphi(m)} \equiv (a, m)^{\varphi(m)} \pmod{m}$$

Proof This fact may be proven the same way as Theorem 3.1, by considering that

$$p_i \mid a \ \Leftrightarrow\ p_i \mid (a,m) \quad (\alpha_i > 0)$$

□

Theorem 3.4

$$|\mathrm{E}_m| = 2^{\omega(m)}$$

Proof From the proof of Theorem 3.1, we see that a number is idempotent modulo m iff it is congruent to either 0 or 1 modulo each of the prime power divisors of m. From this fact, our theorem follows quite clearly, by the application of the Chinese Remainder Theorem (see [1]). □

Theorem 3.5 *For $k \in \mathbb{N}$*

$$|k\mathrm{E}_m \bmod m| = 2^{\omega\left(\frac{m}{(k,m)}\right)}$$

Proof Let

$$\frac{m}{(k,m)} = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

be the prime-factorization of $\frac{m}{(k,m)}$. We see that $\beta_i = 0$ iff $p_i^{\alpha_i} \mid k$, so

$$\omega\left(\frac{m}{(k,m)}\right) = |\{i : \beta_i > 0\}| = |\{i : p_i^{\alpha_i} \nmid k\}|$$

Without hurting generality, we may suppose that p_i are ordered so that for some $n \in \mathbb{N}$ we have $\beta_i > 0$ if $1 \leq i \leq n$ and $\beta_i = 0$ if $i > n$. Let

$$m_1 := \prod_{i=1}^{n} p_i^{\alpha_i}, \quad m_2 := \prod_{i=n+1}^{\infty} p_i^{\alpha_i}$$

This way we have for all $e \in \mathrm{E}_m$ that

$$ke \equiv 0 \text{ or } ke \equiv k \not\equiv 0 \pmod{p_i^{\alpha_i}} \quad (1 \leq i \leq n)$$

and $ke \equiv 0 \pmod{m_2}$. So by the Chinese Remainder Theorem and Theorem 3.4 we have

$$|k\mathrm{E}_m \bmod m| = |k\mathrm{E}_{m_1} \bmod m_1| \cdot |k\mathrm{E}_{m_2} \bmod m_2| = |\mathrm{E}_{m_1}| \cdot |\{0\}| = 2^n = 2^{\omega\left(\frac{m}{(k,m)}\right)}$$

□

Theorem 3.6 *If for some $a \in \mathbb{Z},\ k,l \in \mathbb{N}$, we have $a^k, a^l \in_m \mathrm{E}_m$, then $a^k \equiv a^l \pmod m$.*

Proof

$$a^k \equiv (a^k)^l \equiv a^{kl} \equiv (a^l)^k \equiv a^l \pmod m$$

□

Definition 3.2 *For $a \in \mathbb{Z}$, let its order modulo m to be the smallest $n \in \mathbb{N}$ for which $a^n \in_m \mathrm{E}_m$. Let $|a|_m$ denote this n.*

$$a^0 := a^{|a|_m} \bmod m$$

Furthermore, let the inverse of a be denoted as

$$a^{-1} := a^{|a|_m - 1} \bmod m$$

and for $k \in \mathbb{N}$

$$a^{-k} := (a^{-1})^k \bmod m$$

For $b \in \mathbb{Z}$, if it exists, let $\mathrm{ind}_b^m a$ denote the smallest $k \in \mathbb{N}$, for which $b^k \equiv a \pmod{m}$, and let its existence be denoted as $\exists \mathrm{ind}_b^m a$.

The existence of the above n is guaranteed by Theorem 3.1.

Theorem 3.7 *If for some $a \in \mathbb{Z},\ k, n \in \mathbb{N},\ k \leq n$ we have $a^{k+n} \equiv a^k \pmod{m}$, then $a^n \in_m \mathrm{E}_m$.*

Proof

$$a^{k+n} \equiv a^k \ \Rightarrow\ a^{n-k}a^{k+n} \equiv a^{n-k}a^k \ \Rightarrow\ (a^n)^2 \equiv a^n \pmod{m}$$

so we have that $a^n \in_m \mathrm{E}_m$. □

Theorem 3.8 *If $m_1, m_2 \in \mathbb{N},\ m = [m_1, m_2]$, then*

$$e \in \mathrm{E}_m \ \Leftrightarrow\ e \in_{m_1} \mathrm{E}_{m_1} \text{ and } e \in_{m_2} \mathrm{E}_{m_2}$$

Proof This follows from the fact that a number is idempotent modulo m iff it is congruent to either 0 or 1 modulo each of the prime power divisors of m. □

Problem 3.1 *Defining the sequence of numbers $(a_n)_{n=1}^{\infty}$ recursively with*

$$a_0 := 1,\ a_n := 42^{a_{n-1}}\ (n \in \mathbb{N})$$

what will be the last two digits of a_{100}?

Solution With some calculation, we get the following results

$$a_{100} = 42^{a_{99}},\ |42|_{100} = 20,\ 42^{20} \equiv 76 \pmod{100}$$

$$a_{99} = 42^{a_{98}},\ |42|_{20} = 4,\ 42^4 \equiv 16 \pmod{20}$$

$$a_{98} = 42^{a_{97}},\ |42|_4 = 2,\ 42^2 \equiv 4 \pmod{4}$$

$$a_{97} \equiv 0 \pmod{2} \ \Rightarrow\ a_{98} \equiv 0 \pmod{4} \ \Rightarrow\ a_{99} \equiv 16 \pmod{20} \ \Rightarrow$$

$$\Rightarrow a_{100} \equiv 76 \cdot 42^{16} \equiv 76 \cdot 56 \equiv 56 \pmod{100}$$

□

Note that the above problem may be solved in other ways as well. I decided to include it in our discussion, because this idea of a solution made me realize the importance of idempotent numbers when discussing composite moduli, and it also gave me incentive to investigate composite moduli from the viewpoint of idempotent numbers, starting the research which resulted in this paper.

4 Normal Numbers

Definition 4.1 *$a \in \mathbb{Z}$ is said to be normal modulo m if the following logical inference holds*

$$a^k \in_m \mathrm{E}_m \;\Rightarrow\; |a|_m \mid k \quad (k \in \mathbb{N})$$

Let N_m denote the subset of normal numbers in $\mathbb{Z}_m$.
Furthermore, for $e \in \mathrm{E}_m$, let N_m^e denote the set

$$\{a \in \mathrm{N}_m : \; a^{|a|_m} \equiv e \pmod m\}$$

Theorem 4.1 *A number $a \in \mathbb{Z}_m$ is normal iff the following logical inference holds*

$$a^k \equiv a^l \pmod m \;\Rightarrow\; k \equiv l \pmod{|a|_m} \quad (k, l \in \mathbb{N})$$

Proof First, let us suppose that $a \in \mathbb{Z}_m$ is normal. Then

$$a^k \equiv a^l \;\Rightarrow\; a^k a^{l\varphi(m)-l} \equiv a^{l\varphi(m)} \pmod m$$

Since $a^{l\varphi(m)} \in_m \mathrm{E}_m$ and $|a|_m \mid \varphi(m)$, we have

$$0 \equiv k + l\varphi(m) - l \equiv k - l \;\Rightarrow\; k \equiv l \pmod{|a|_m}$$

Now, if the inference holds, with $l := |a|_m$ we have that a is normal. □

Theorem 4.2 *If $m_1, m_2 \in \mathbb{N}$, $m_1 \mid m_2$, $a \in \mathrm{N}_{m_1}$, then $|a|_{m_1} \mid |a|_{m_2}$.*

Proof

$$a^{|a|_{m_2}} \in_{m_2} \mathrm{E}_{m_2},\; m_1 \mid m_2 \;\Rightarrow\; a^{|a|_{m_2}} \in_{m_1} \mathrm{E}_{m_1},\; a \in \mathrm{N}_{m_1} \;\Rightarrow\; |a|_{m_1} \mid |a|_{m_2}$$

□

Theorem 4.3 *Let $m_1, m_2 \in \mathbb{N}$ be such that $m = [m_1, m_2]$, and $a \in \mathbb{Z}_m$. If $a \in_{m_1} \mathrm{N}_{m_1}$ and $a \in_{m_2} \mathrm{N}_{m_2}$, then $a \in \mathrm{N}_m$ and $|a|_m = [|a|_{m_1}, |a|_{m_2}]$.*

Proof By Theorem 3.8, for $k \in \mathbb{N}$ we have

$$a^k \in_m \mathrm{E}_m \;\Leftrightarrow a^k \in_{m_1} \mathrm{E}_{m_1},\; a^k \in_{m_2} \mathrm{E}_{m_2} \;\Rightarrow\; [|a|_{m_1}, |a|_{m_2}] \mid k$$

so $[|a|_{m_1}, |a|_{m_2}] \mid |a|_m$. With $k = [|a|_{m_1}, |a|_{m_2}]$ we have $a^{[|a|_{m_1}, |a|_{m_2}]} \in_m \mathrm{E}_m$ so $|a|_m \leq [|a|_{m_1}, |a|_{m_2}]$, so $|a|_m = [|a|_{m_1}, |a|_{m_2}]$. We also see from above that a is normal modulo m. □

Theorem 4.4 *If $a \in \mathrm{N}_m$, $k \in \mathbb{N}$ then*

$$|a^k|_m = \frac{|a|_m}{(k, |a|_m)}$$

Proof

$$(a^k)^{\frac{|a|_m}{(k,|a|_m)}} \equiv (a^{|a|_m})^{\frac{k}{(k,|a|_m)}} \in_m \mathrm{E}_m$$

so we have

$$|a^k|_m \le \frac{|a|_m}{(k, |a|_m)}$$

by Definition 3.2.

$$a^{kl} \in_m \mathrm{E}_m \;\Rightarrow\; |a|_m \mid kl \;\Leftrightarrow\; \frac{|a|_m}{(k, |a|_m)} \mid l$$

so we have

$$|a^k|_m \ge \frac{|a|_m}{(k, |a|_m)}$$

□

Theorem 4.5 *If $a \in \mathrm{N}_m,\ n \in \mathbb{N}$, then $a^n \in_m \mathrm{N}_m$.*

Proof For all $k \in \mathbb{N}$

$$(a^n)^k \in_m \mathrm{E}_m \;\Rightarrow\; |a|_m \mid nk \;\Leftrightarrow\; |a^n|_m = \frac{|a|_m}{(n, |a|_m)} \mid k$$

□

Theorem 4.6 *Let $e \in \mathrm{E}_m,\ a, b \in \mathrm{N}^e_m,\ k \in \mathbb{N}$ be such that $\exists \mathrm{ind}^m_b a$. Then*

$$a^{\frac{|b|_m}{(k,|b|_m)}} \in_m \mathrm{E}_m \;\Rightarrow\; (k, |b|_m) \mid \mathrm{ind}^m_b a$$

Proof

$$e \equiv a^{\frac{|b|_m}{(k,|b|_m)}} \equiv b^{\frac{|b|_m \mathrm{ind}^m_b a}{(k,|b|_m)}} \pmod{m} \;\Rightarrow$$

$$\Rightarrow\; |b|_m \mid \frac{|b|_m \mathrm{ind}^m_b a}{(k, |b|_m)} \;\Leftrightarrow\; \frac{\mathrm{ind}^m_b a}{(k, |b|_m)} \in \mathbb{Z} \;\Leftrightarrow\; (k, |b|_m) \mid \mathrm{ind}^m_b a$$

□

Theorem 4.7 *For all $a \in \mathrm{N}_m$ we have $a^{-1} \in \mathrm{N}_m,\ |a^{-1}|_m = |a|_m$ and*

$$(a^{-1})^{-1} \equiv a^{|a|_m+1} \pmod{m}$$

Proof The first statement follows from Theorem 4.5. The second statement follows from Theorems 4.5 and 4.4 since

$$|a^{|a|_m-1}|_m = \frac{|a|_m}{(|a|_m - 1, |a|_m)} = |a|_m$$

If $|a|_m \ge 2$ then

$$(a^{-1})^{-1} \equiv (a^{|a|_m-1})^{|a|_m-1} \equiv a \cdot (a^{|a|_m})^{|a|_m-2} \pmod{m}$$

The case of $a \in \mathrm{E}_m$ is trivial. □

5 Regular Numbers

Definition 5.1 *$a \in \mathbb{Z}$ is said to be regular modulo m if*

$$a^{|a|_m+1} \equiv a \pmod{m}$$

Let R_m denote the subset of regular numbers in $\mathbb{Z}_m$.
Furthermore, for $e \in \mathrm{E}_m$, let R_m^e denote the set

$$\{a \in \mathrm{R}_m : \ a^{|a|_m} \equiv e \pmod{m}\}$$

From Theorems 3.1 and 3.6 we have that for all $a \in \mathbb{Z}$

$$a^{|a|_m} \equiv a^{\varphi(m)} \pmod{m}$$

We will apply this simple fact in our next theorem.

Theorem 5.1

$$\mathrm{R}_m = \mathbb{Z}_m$$

iff m is square-free.

Proof First, let us suppose that $\mathrm{R}_m = \mathbb{Z}_m$. Then for all $i : \alpha_i > 0$ we have

$$p_i(p_i^{\varphi(m)} - 1) \equiv 0 \pmod{m} \ \Rightarrow \ p_i(p_i^{\varphi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}} \ \Rightarrow \ \alpha_i = 1$$

Now, if m is square-free, then for all $a \in \mathbb{Z}_m$

$$a(a^{\varphi(m)} - 1) \equiv 0 \pmod{p_i} \ (i \in \mathbb{N}) \ \Rightarrow \ a(a^{\varphi(m)} - 1) \equiv 0 \pmod{m}$$

□

Theorem 5.2

$$\mathrm{R}_m \subset \mathrm{N}_m$$

Proof We need to show that for all $a \in \mathrm{R}_m$, if $a^k \in_m \mathrm{E}_m$ then $|a|_m \mid k$ for all $k \in \mathbb{N}$. Let $q, r \in \mathbb{N} \cup \{0\}$ be such that

$$k = q|a|_m + r, \ 0 \leq r < |a|_m$$

Let us suppose that $r > 0$. Then we have

$$a^r \equiv a \cdot a^{r-1} \equiv a^{|a|_m+1} \cdot a^{r-1} \equiv (a^{|a|_m})^q \cdot a^r \equiv a^k \pmod{m}$$

so $a^r \in_m \mathrm{E}_m$, which is a contradiction by Definition 3.2. □

Theorem 5.3 *For all $e \in \mathrm{E}_m$*

$$\mathrm{R}_m^e = \{ea \bmod m : \ a^{|a|_m} \equiv e \pmod{m}, \ a \in \mathbb{Z}_m\}$$

Proof If $a \in \mathrm{R}_m^e$ then $a \equiv e \cdot a \pmod{m}$ which is obviously in the set on the right-hand side. Now if $a \in \mathbb{Z}_m$ is such that $a^{\varphi(m)} \equiv e \pmod{m}$, then multiplying this congruence by ea we have

$$(ea)(ea)^{\varphi(m)} \equiv ea \pmod{m}$$

so $ea \in_m \mathrm{R}^e_m$. □

Theorem 5.4 *For all* $a \in \mathbb{Z}$

$$a^m \equiv a^{m-\varphi(m)} \equiv a^{m+\varphi(m)} \pmod{m}$$

and

$$a^{m-\varphi(m)} \in_m \mathrm{R}_m$$

Furthermore

$$a^{\varphi(m)-1} \in_m \mathrm{R}_m$$

if $|a|_m < \varphi(m)$ *and* $a \in \mathrm{N}_m$.

Proof Let $i \in \mathbb{N}$ be a fixed number, and $\alpha_i > 0$. There are two possibilities.
1. $p_i \mid a$

$$\alpha_i \le p_i^{\alpha_i - 1} \le p_i^{\alpha_i - 1} \cdot q = m - \varphi(m)$$

for some $q \in \mathbb{N}$, so

$$a^{m-\varphi(m)} \equiv 0 \pmod{p_i^{\alpha_i}}$$

2. $p_i \nmid a$
In this case we have

$$a^{\varphi(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$$

In both cases 1. and 2., we have

$$a^{m-\varphi(m)}(a^{\varphi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}}$$

from which we have our first congruence. The second one follows easily, by multiplying both sides by $a^{\varphi(m)}$.

$$a^{m-\varphi(m)} \cdot (a^{m-\varphi(m)})^{\varphi(m)} \equiv a^{m-\varphi(m)} \cdot a^{\varphi(m)} = a^m \equiv a^{m-\varphi(m)} \pmod{m}$$

From Theorem 5.2, and the definition of normal numbers, we have that $\varphi(m) = k|a|_m$ for some $k > 1$. So

$$a^{\varphi(m)-1} \cdot (a^{\varphi(m)-1})^{\varphi(m)} \equiv a^{\varphi(m)-1} \cdot a^{\varphi(m)} \equiv$$

$$\equiv a^{\varphi(m)} \cdot a^{|a|_m} \cdot a^{(k-1)|a|_m - 1} \equiv a^{|a|_m} \cdot a^{(k-1)|a|_m - 1} = a^{\varphi(m)-1} \pmod{m}$$

□

Note that based on our previous theorem, we may define the function

$$\delta_m(a) := \min\{n \in \mathbb{N} : \ a^n \in_m \mathrm{R}_m\} \quad (a \in \mathbb{Z}_m)$$

which has the property

$$\delta_m(a) = \min\{n \in \mathbb{N} : \ a^{|a|_m + n} \equiv a^n \pmod{m}\}$$

since

$$a^n \in_m \mathrm{R}_m \;\Leftrightarrow\; a^{|a|_m+n} \equiv a^n \pmod{m}$$

Theorem 5.5 *A number $a \in \mathbb{Z}_m$ is regular iff the following logical inference holds*

$$p_i \mid a \;\Rightarrow\; p_i^{\alpha_i} \mid a \quad (i \in \mathbb{N},\; \alpha_i > 0)$$

Proof If $a \in \mathrm{R}_m$ then $a \cdot a^{\varphi(m)} \equiv a \pmod{m}$. Let $i \in \mathbb{N}$ be such that $\alpha_i > 0$, and suppose that $p_i \mid a$. Then as in the proof of Theorem 3.1, we have

$$a \equiv a \cdot a^{\varphi(m)} \equiv a \cdot 0 \equiv 0 \pmod{p_i^{\alpha_i}}$$

Now, let us suppose that the inference holds. Let $i \in \mathbb{N}$ be such that $\alpha_i > 0$. There are two possible cases.
1. $p_i \mid a$
Then we know that $p_i^{\alpha_i} \mid a$ is true as well, so

$$a \cdot a^{\varphi(m)} \equiv 0 \equiv a \pmod{p_i^{\alpha_i}}$$

2. $p_i \nmid a$
In this case we have $(a, p_i^{\alpha_i}) = 1$, so

$$a \cdot a^{\varphi(m)} \equiv a \pmod{p_i^{\alpha_i}}$$

From these two cases we have that $a \in \mathrm{R}_m$. □

Theorem 5.6 *A number $a \in \mathbb{Z}_m$ is regular iff the following equivalence holds*

$$a^k \equiv a^l \pmod{m} \;\Leftrightarrow\; k \equiv l \pmod{|a|_m} \quad (k, l \in \mathbb{N})$$

It is also true that if $a \in \mathbb{Z}_m$ is regular, then the following equivalence holds

$$a^k \in_m \mathrm{E}_m \;\Leftrightarrow\; |a|_m \mid k \quad (k \in \mathbb{N})$$

Proof Let us first suppose that $a \in \mathbb{Z}_m$ is regular. The $\Rightarrow$ part of the equivalence follows from Theorems 4.1 and 5.2. The $\Leftarrow$ part is also true, since if $l \geq k$ and $k \equiv l \pmod{|a|_m}$, then for some $q \geq 0$, we have $l = k + q|a|_m$, so

$$a^l \equiv a^{k+q|a|_m} \equiv a^k a^{|a|_m} \equiv a^k \pmod{m}$$

where the last congruence holds, because a is regular.
Let us now suppose that the equivalence holds. Then, with $k := |a|_m + 1,\; l := 1$, we have that a is regular.
The second equivalence follows easily from the first. □

Theorem 5.7 *A number $a \in \mathbb{Z}_m$ is regular iff there exists some $n > 1$ such that*

$$a^n \equiv a \pmod{m}$$

Proof First, let us suppose that such an n exists. Then by Theorem 3.7 we have $a^{n-1} \in_m \mathrm{E}_m$, from which $a^{n-1} \equiv a^{|a|_m} \pmod{m}$ follows by the application of Theorem

3.6. So, by multiplying this congruence by a, we get our desired result. Now, supposing that a is regular, we may take $n := |a|_m + 1$. □

Theorem 5.8 *For $a \in \mathbb{Z}_m$*

$$a \in \mathrm{R}_m \;\Leftrightarrow\; \left(a, \frac{m}{(a,m)}\right) = 1 \;\Leftrightarrow\; (a,m) \in \mathrm{R}_m$$

Proof The first equivalence follows clearly from Theorem 5.5. Using this, and the fact that

$$\left((a,m), \frac{m}{((a,m),m)}\right) = \left(a, \frac{m}{(a,m)}\right)$$

we get the second equivalence. □

Theorem 5.9 *For all $a \in \mathrm{N}_m$*

$$a \in \mathrm{R}_m \;\Leftrightarrow\; (a^{-1})^{-1} \equiv a \pmod{m}$$

Proof Follows from Theorem 4.7. □

Theorem 5.10 *Let $m_1, m_2 \in \mathbb{N}$ be such that $m = [m_1, m_2]$, and $a \in \mathbb{Z}_m$. Then*

$$a \in \mathrm{R}_m \;\Leftrightarrow\; a \in_{m_1} \mathrm{R}_{m_1} \text{ and } a \in_{m_2} \mathrm{R}_{m_2}$$

Furthermore, if $a \in \mathrm{R}_m$ then $|a|_m = [|a|_{m_1}, |a|_{m_2}]$.

Proof We will prove the equivalence using Theorem 5.5. Let us suppose that m_1 and m_2 have prime-factorizations

$$m_1 = \prod_{i=1}^{\infty} p_i^{\beta_i}, \quad m_2 = \prod_{i=1}^{\infty} p_i^{\gamma_i}$$

Then we have that $\alpha_i = \max(\beta_i, \gamma_i)$ for all $i \in \mathbb{N}$, since $m = [m_1, m_2]$.
The $\Rightarrow$ part: Taking any i such that $p_i \mid a$, we have $p_i^{\alpha_i} \mid a$, which implies $p_i^{\beta_i} \mid a$ and $p_i^{\gamma_i} \mid a$, since $\alpha_i = \max(\beta_i, \gamma_i)$, so $a \in_{m_1} \mathrm{R}_{m_1}$ and $a \in_{m_2} \mathrm{R}_{m_2}$.
The $\Leftarrow$ part: Taking any i such that $p_i \mid a$, we have $p_i^{\beta_i} \mid a$ and $p_i^{\gamma_i} \mid a$, which implies $p_i^{\alpha_i} \mid a$, so we have that $a \in \mathrm{R}_m$.
Now, let us suppose that $a \in \mathrm{R}_m$. By Theorem 3.8, for $k \in \mathbb{N}$ we have

$$a^k \in_m \mathrm{E}_m \;\Leftrightarrow a^k \in_{m_1} \mathrm{E}_{m_1},\; a^k \in_{m_2} \mathrm{E}_{m_2} \;\Leftrightarrow\; [|a|_{m_1}, |a|_{m_2}] \mid k$$

From this we have that $[|a|_{m_1}, |a|_{m_2}] \mid |a|_m$. With $k = [|a|_{m_1}, |a|_{m_2}]$ we have $a^{[|a|_{m_1}, |a|_{m_2}]} \in_m \mathrm{E}_m$ so $|a|_m \leq [|a|_{m_1}, |a|_{m_2}]$, so $|a|_m = [|a|_{m_1}, |a|_{m_2}]$. □

Theorem 5.11 *For $e \in \mathrm{E}_m$, there exist unique $m_1, m_2 \in \mathbb{N}$ such that $m = m_1 m_2$ and*

$$e \equiv 1 \pmod{m_1} \text{ and } e \equiv 0 \pmod{m_2}$$

Furthermore, for all $a \in \mathbb{Z}_m$, the following equivalence holds

$$a \in \mathrm{R}_m^e \;\Leftrightarrow\; (a, m_1) = 1 \text{ and } m_2 \mid a$$

and if $a \in \mathrm{R}_m^e$ *then* $|a|_m = |a|_{m_1}$.

Proof The proof is quite trivial, with the previous theorem in mind. □

Definition 5.2 *For* $a \in \mathbb{Z}_m$, $a^{\varphi(m)} \equiv e \pmod m$, *using the notations of the theorem above, denote* $\mu_m(a) := m_1$.

We advise the reader to observe throughout our paper, that in many cases it is sufficient to examine the set $\mathrm{R}^1_{\mu_m(e)}$ instead of R_m^e (for any $e \in \mathrm{E}_m$).

Theorem 5.12 *For* $a \in \mathbb{Z}_m$

$$a \in \mathrm{R}_m \;\Leftrightarrow\; a \in_{p_i^{\alpha_i}} \mathrm{R}_{p_i^{\alpha_i}} \quad (i \in \mathbb{N})$$

and, if $a \in \mathrm{R}_m$ *then*

$$|a|_m = \mathrm{lcm}(|a|_{p_i^{\alpha_i}} : 1 \le i \le \infty)$$

Furthermore,

$$|\mathrm{R}_m| = \prod_{\alpha_i > 0} (1 + \varphi(p_i^{\alpha_i}))$$

Proof Follows from Theorem 5.10.
The formula for $|\mathrm{R}_m|$ follows from the fact that for $a \in \mathbb{Z}_{p_i^{\alpha_i}}$

$$a \in \mathrm{R}_{p_i^{\alpha_i}} \;\Leftrightarrow\; p_i \nmid a \text{ or } p_i^{\alpha_i} \mid a$$

which is a consequence of Theorem 5.5. □

Theorem 5.13 *For all* $e \in \mathrm{E}_m$, *the structure* $\langle \mathrm{R}_m^e; \{e, ^{-1}, \cdot\}\rangle$ *is an Abelian group.*

Proof The properties to be shown are mostly trivial, except for maybe one. We need to show that for all $a \in \mathrm{R}_m^e$ there exists a unique $b \in \mathrm{R}_m^e$ such that $ab \equiv e \pmod m$. Let $b := a^{-1}$. It is obvious that $b \in \mathrm{R}_m^e$ and $ab \equiv e \pmod m$. Now, let us suppose that there exists some other $b' \in \mathrm{R}_m^e$ such that $ab' \equiv e \pmod m$. Then we have

$$a(b - b') \equiv 0 \pmod m \;\Rightarrow\; 0 \equiv a^{|a|_m - 1} \cdot a(b - b') \equiv$$

$$\equiv e(b - b') \equiv b^{|b|_m + 1} - (b')^{|b'|_m + 1} \equiv b - b' \pmod m$$

□

Theorem 5.14 *If* m *is an odd number, then for all* $e \in \mathrm{E}_m$

$$\prod \mathrm{R}_m^e \equiv (-1)^{2^{\omega(\mu_m(e)) - 1}} \cdot e \pmod m$$

Proof We are going to make use of Theorem 10.5 from the last section, which states that

$$\prod \{a \in \mathrm{R}_m^e : |a|_m \le 2\} \equiv (-1)^{2^{\omega(\mu_m(e)) - 1}} \cdot e \pmod m$$

For now, denote

$$S := \{a \in \mathrm{R}_m^e : |a|_m \le 2\}$$

Then for all $a \in \mathrm{R}_m^e$

$$a \ne a^{-1} \;\Leftrightarrow\; a \in \mathrm{R}_m^e \setminus S$$

By our previous theorem, we have that

$$\prod \mathrm{R}_m^e \setminus S \equiv e \pmod{m}$$

So we have

$$\prod \mathrm{R}_m^e \equiv \left(\prod \mathrm{R}_m^e \setminus S\right) \cdot \left(\prod S\right) \equiv e \cdot (-1)^{2^{\omega(\mu_m(e))-1}} \cdot e \pmod{m}$$

□

Theorem 5.15 *For* $a \in \mathrm{R}_m,\ n \in \mathbb{N},\ i, j \in \mathbb{Z}$

$$(a^n)^{-1} \equiv a^{-n} \pmod{m}$$

$$a^{i+j} \equiv a^i \cdot a^j \pmod{m}$$

Proof The first statement is equivalent to saying that

$$a^{n\frac{|a|_m}{(n,|a|_m)}-n} \equiv a^{n|a|_m - n} \pmod{m}$$

which by Theorem 5.6 is equivalent to

$$n\frac{|a|_m}{(n,|a|_m)} - n \equiv n|a|_m - n \pmod{|a|_m}$$

(when $n\frac{|a|_m}{(n,|a|_m)} - n \neq 0$), and this congruence obviously holds.
In the omitted case

$$n\frac{|a|_m}{(n,|a|_m)} - n = 0 \ \Leftrightarrow\ |a|_m \mid n$$

So for some $k \in \mathbb{N}$, we have

$$a^{n|a|_m - n} = a^{(n-k)|a|_m} \equiv a^0 \pmod{|a|_m}$$

For the second property, we can distinguish four different cases (for nonzero exponents).
Case of $i, j < 0$:

$$a^{i+j} = a^{-|i+j|} \equiv (a^{-1})^{|i+j|} = (a^{-1})^{|i|} \cdot (a^{-1})^{|j|} \equiv$$
$$\equiv a^{-|i|} \cdot a^{-|j|} \equiv a^i \cdot a^j \pmod{m}$$

Case of $i < 0,\ j > 0$:
Case of $j \geq |i|$*:*

$$a^{i+j} = a^{j-|i|} \ \Rightarrow\ a^j = a^{i+j} \cdot a^{|i|} \ \Rightarrow$$
$$\Rightarrow a^{i+j} \equiv a^j \cdot (a^{|i|})^{-1} \equiv a^j \cdot a^{-|i|} = a^i \cdot a^j \pmod{m}$$

Case of $j < |i|$*:*

$$a^{i+j} \equiv a^{j-|i|} \equiv a^{-(|i|-j)} \equiv (a^{|i|-j})^{-1} \equiv (a^{|i|} \cdot a^{-j})^{-1} \pmod{m}$$

where the last congruence is true with the application of the previous case.

$$(a^{|i|} \cdot a^{-j}) \cdot (a^{-|i|} \cdot a^j) \equiv (a^{|i|})(a^{|i|})^{-1}(a^j)^{-1}(a^j) \equiv (a^{|a|_m})^{|i|+j} \equiv a^{|a|_m} \pmod{m}$$

So by the unicity of the inverse (Theorem 5.13), we have

$$(a^{|i|} \cdot a^{-j})^{-1} \equiv a^{-|i|} \cdot a^{j} \equiv a^{i} \cdot a^{j} \pmod{m}$$

Case of $i, j > 0$ is trivial.
Case of $i > 0,\ j < 0$ is similar to the case of $i < 0,\ j > 0$. □

Definition 5.3 *For $a \in \mathbb{Z}_m$, let $\langle a \rangle_m$ denote the set*

$$\{a^n \bmod m : \ 1 \leq n \leq |a|_m\}$$

and in case of $A \subset \mathbb{Z}_m$, let $\langle A \rangle_m$ denote the set

$$\bigcup_{a \in A} \langle a \rangle_m$$

Theorem 5.16 *Let $b, c \in \mathrm{R}_m,\ n, k \in \mathbb{N}$. Then*

$$b^n, b^k \in_m \langle c \rangle_m \ \Leftrightarrow \ b^{(n,k)} \in_m \langle c \rangle_m$$

Proof Let us first suppose that $b^n \equiv c^i,\ b^k \equiv c^j \pmod{m}$. Without hurting generality, we may suppose that there exist $x, y \geq 0$ such that $(n, k) = nx - ky$. So we have

$$b^{(n,k)} = b^{nx-ky} = b^{nx+(-ky)} \equiv b^{nx} \cdot b^{-ky} \equiv b^{nx} \cdot (b^{ky})^{-1} \equiv (c^{ix}) \cdot (c^{jy})^{\varphi(m)-1} \in_m \langle c \rangle_m$$

with the application of Theorem 5.15.
Now, let us suppose that $b^{(n,k)} \equiv c^l \pmod{m}$. Then we have

$$b^n \equiv b^{(n,k)\frac{n}{(n,k)}} \equiv (c^l)^{\frac{n}{(n,k)}} \in_m \langle c \rangle_m$$

The proof is similar for $b^k \in_m \langle c \rangle_m$. □

Definition 5.4 *For $e \in \mathrm{E}_m,\ b, c \in \mathrm{R}^e_m$, denote*

$$\mathrm{D}_m(b, c) := \gcd(n \in \mathbb{N} : \ 1 \leq n \leq |b|_m,\ b^n \in_m \langle c \rangle_m)$$

Theorem 5.17 *If $e \in \mathrm{E}_m,\ b, c \in \mathrm{R}^e_m$, then $\mathrm{D}_m(b, c) \mid |b|_m$ and*

$$b^k \in_m \langle c \rangle_m \ \Leftrightarrow \ \mathrm{D}_m(b, c) \mid k$$

It is also true that $b^{\mathrm{D}_m(b,c)} \in_m \langle c \rangle_m$ and

$$\langle b \rangle_m \cap \langle c \rangle_m = \langle b^{\mathrm{D}_m(b,c)} \rangle_m$$

Furthermore

$$|\langle b \rangle_m \cap \langle c \rangle_m| = \frac{|b|_m}{\mathrm{D}_m(b, c)}$$

Proof By Theorem 5.16 and with induction, we have $b^{\mathrm{D}_m(b,c)} \in_m \langle c \rangle_m$.
First, let us suppose that $\mathrm{D}_m(b, c) \mid k$. Then we have

$$b^k \equiv (b^{\mathrm{D}_m(b,c)})^{\frac{k}{\mathrm{D}_m(b,c)}} \in_m \langle c \rangle_m$$

Now, if $b^k \in_m \langle c\rangle_m$ then with $k' := k \bmod |b|_m$, we have $b^{k'} \in_m \langle c\rangle_m$, so $\mathrm{D}_m(b,c) \mid k'$ by definition, and from this it follows that $\mathrm{D}_m(b,c) \mid k$.
So by the property now proven, we also have that

$$\langle b\rangle_m \cap \langle c\rangle_m = \langle b^{\mathrm{D}_m(b,c)}\rangle_m$$

It is also true that $\mathrm{D}_m(b,c) \mid |b|_m$ since

$$b^{|b|_m} \equiv e \equiv c^{|c|_m} \in_m \langle c\rangle_m$$

So we have

$$|\langle b\rangle_m \cap \langle c\rangle_m| = |\langle b^{\mathrm{D}_m(b,c)}\rangle_m| = |b^{\mathrm{D}_m(b,c)}|_m = \frac{|b|_m}{(\mathrm{D}_m(b,c), |b|_m)} = \frac{|b|_m}{\mathrm{D}_m(b,c)}$$

□

Theorem 5.18 *Let* $k \in \mathbb{N},\ e \in \mathrm{E}_m,\ a,b \in \mathrm{R}^e_m,\ \exists \mathrm{ind}^m_b a$. *Then*

$$(k, |b|_m) \mid \mathrm{ind}^m_b a \ \Leftrightarrow\ a^{\frac{|b|_m}{(k,|b|_m)}} \in_m \mathrm{E}_m$$

Proof

$$e \equiv a^{\frac{|b|_m}{(k,|b|_m)}} \equiv b^{\frac{|b|_m \mathrm{ind}^m_b a}{(k,|b|_m)}} \pmod m \ \Leftrightarrow$$

$$\Leftrightarrow\ |b|_m \mid \frac{|b|_m \mathrm{ind}^m_b a}{(k,|b|_m)} \ \Leftrightarrow\ \frac{\mathrm{ind}^m_b a}{(k,|b|_m)} \in \mathbb{Z} \ \Leftrightarrow\ (k,|b|_m) \mid \mathrm{ind}^m_b a$$

□

Theorem 5.19 *For* $e \in \mathrm{E}_m,\ a,b \in \mathrm{R}^e_m$

$$(|a|_m, |b|_m) = 1 \ \Leftrightarrow\ |ab|_m = |a|_m \cdot |b|_m$$

$$\frac{[|a|_m, |b|_m]}{(|a|_m, |b|_m)} \mid |ab|_m \mid [|a|_m, |b|_m]$$

$$a^{|b|_m} \equiv b^{|a|_m} \pmod m \ \Rightarrow\ |a|_m = |b|_m$$

Proof We first prove the second property.

$$(ab)^{[|a|_m,|b|_m]} \equiv e \pmod m \ \Rightarrow\ |ab|_m \mid [|a|_m, |b|_m]$$

$$e \equiv (ab)^{|a|_m \cdot |ab|_m} \equiv e \cdot b^{|a|_m \cdot |ab|_m} \equiv b^{|a|_m \cdot |ab|_m} \pmod m \ \Rightarrow$$

$$\Rightarrow\ |b|_m \mid |a|_m \cdot |ab|_m \ \Rightarrow\ \frac{|b|_m}{(|a|_m, |b|_m)} \mid |ab|_m$$

$$e \equiv (ab)^{|b|_m \cdot |ab|_m} \equiv e \cdot a^{|b|_m \cdot |ab|_m} \equiv a^{|b|_m \cdot |ab|_m} \pmod m \ \Rightarrow$$

$$\Rightarrow\ |a|_m \mid |b|_m \cdot |ab|_m \ \Rightarrow\ \frac{|a|_m}{(|a|_m, |b|_m)} \mid |ab|_m$$

$$\Rightarrow\ \left[\frac{|a|_m}{(|a|_m, |b|_m)}, \frac{|b|_m}{(|a|_m, |b|_m)}\right] = \frac{[|a|_m, |b|_m]}{(|a|_m, |b|_m)} \mid |ab|_m$$

The first property follows from the second one.
Now, we prove the third one.

$$e \equiv a^{|b|_m \frac{|a|_m}{(|a|_m,|b|_m)}} \equiv b^{\frac{|a|_m^2}{(|a|_m,|b|_m)}} \pmod{m} \Rightarrow$$

$$\Rightarrow |b|_m \mid |a|_m \frac{|a|_m}{(|a|_m,|b|_m)} \Leftrightarrow \frac{|b|_m}{(|a|_m,|b|_m)} \mid \frac{|a|_m}{(|a|_m,|b|_m)} \Rightarrow |b|_m \mid |a|_m$$

We get $|a|_m \mid |b|_m$ the same way. □

Theorem 5.20 *Suppose that* $e \in \mathrm{E}_m$, $a, b, c \in \mathrm{R}_m^e$ *and* $a \in \langle b\rangle_m \cap \langle c\rangle_m$. *Then there exists some* $d \in \mathrm{R}_m^e$ *for which* $a \in \langle d\rangle_m$ *and* $|d|_m = [|b|_m, |c|_m]$.

Proof By Theorem 5.17, we have

$$\langle b\rangle_m \cap \langle c\rangle_m = \langle b^{\mathrm{D}_m(b,c)}\rangle_m = \langle c^{\mathrm{D}_m(c,b)}\rangle_m$$

so there exists some $K \in \mathbb{N}$ such that

$$(b^{\mathrm{D}_m(b,c)})^K \equiv c^{\mathrm{D}_m(c,b)} \pmod{m}$$

and from

$$|b^{\mathrm{D}_m(b,c)}|_m = |\langle b\rangle_m \cap \langle c\rangle_m| = |c^{\mathrm{D}_m(c,b)}|_m = \frac{|b^{\mathrm{D}_m(b,c)}|_m}{(K, |b^{\mathrm{D}_m(b,c)}|_m)}$$

we have $(K, |b^{\mathrm{D}_m(b,c)}|_m) = 1$.

$$\frac{|b|_m}{\mathrm{D}_m(b,c)} = \frac{|c|_m}{\mathrm{D}_m(c,b)} \Rightarrow \mathrm{D}_m(c,b)\frac{|b|_m}{(|b|_m,|c|_m)} = \mathrm{D}_m(b,c)\frac{|c|_m}{(|b|_m,|c|_m)}$$

$$\Rightarrow \frac{|b|_m}{(|b|_m,|c|_m)} \mid \mathrm{D}_m(b,c)\frac{|c|_m}{(|b|_m,|c|_m)}$$

and since

$$\left(\frac{|b|_m}{(|b|_m,|c|_m)}, \frac{|c|_m}{(|b|_m,|c|_m)}\right) = 1$$

we have

$$\frac{|b|_m}{(|b|_m,|c|_m)} \mid \mathrm{D}_m(b,c)$$

Denote

$$l := \frac{\mathrm{D}_m(b,c)(|b|_m,|c|_m)}{|b|_m}$$

$$|b|_m = n_1 n_2 n_3,\ |c|_m = k_1 k_2 k_3,\ l = l_1 l_2$$

where the numbers above have the properties

$$k_1 \mid n_1,\ n_2 \mid k_2,\ l_1 \mid n_2,\ l_2 \mid k_1$$

$$1 = (n_3, k_3) = (n_i, n_j) = (n_i, k_j) = (k_i, k_j) \quad (i \neq j)$$

Then we have

$$(|b|_m, |c|_m) = n_2 k_1,\ |b^{n_2}|_m = n_1 n_3,\ |c^{k_1}|_m = k_2 k_3,\ (|b^{n_2}|_m, |c^{k_1}|_m) = 1$$

and also

$$\mathrm{D}_m(b,c) = l\frac{n_1}{k_1}n_3,\ \mathrm{D}_m(c,b) = l\frac{k_2}{n_2}k_3,\ |b^{\mathrm{D}_m(b,c)}|_m = \frac{n_2k_1}{l}$$

So by Theorem 5.19

$$|b^{n_2}c^{k_1}|_m = n_1n_3k_2k_3 = [|b|_m, |c|_m]$$

Denote $d := b^{n_2}c^{k_1} \bmod m$.

$$d^{l\frac{n_1k_2}{k_1n_2}n_3k_3} \equiv (b^{\mathrm{D}_m(b,c)})^{k_2k_3}(c^{\mathrm{D}_m(c,b)})^{n_1n_3} \equiv (b^{\mathrm{D}_m(b,c)})^{k_2k_3+Kn_1n_3} \pmod m$$

$$(k_2k_3 + Kn_1n_3, \frac{n_2k_1}{l_1l_2}) = 1$$

since $\frac{n_2}{l_1} \mid k_2$ but $(\frac{n_2}{l_1}, Kn_1n_3) = 1$, and $\frac{k_1}{l_2} \mid n_1$ but $(\frac{k_1}{l_2}, k_2k_3) = 1$.
So there exists some $N \in \mathbb{N}$, such that

$$(k_2k_3 + Kn_1n_3)N \equiv 1 \ (\mathrm{mod}\ \frac{n_2k_1}{l})$$

So since $(b^{\mathrm{D}_m(b,c)})^I \equiv a \pmod m$ for some $I \in \mathbb{N}$, we have

$$d^{l\frac{n_1k_2}{k_1n_2}n_3k_3NI} \equiv (b^{\mathrm{D}_m(b,c)})^{(k_2k_3+Kn_1n_3)NI} \equiv (b^{\mathrm{D}_m(b,c)})^I \equiv a \pmod m$$

So $a \in \langle d\rangle_m$. □

Theorem 5.21 *Let $e \in \mathrm{E}_m,\ a \in \mathrm{R}^e_m,\ b \in \mathrm{N}_m$ be such that $a \in \langle b\rangle_m$. Then there exists some $c \in \mathrm{R}^e_m$ such that $a \in \langle c\rangle_m$ and $|c|_m = |b|_m$.*

Proof Define $c := be \bmod m$. Then obviously $c \in \mathrm{R}^e_m$, and

$$c^{\mathrm{ind}^m_b a} \equiv b^{\mathrm{ind}^m_b a} \cdot e \equiv a \cdot e \equiv a \pmod m$$

So $a \in \langle c\rangle_m$. Since $b^{|b|_m} \equiv e \pmod m$, we have $c \equiv b^{|b|_m+1} \pmod m$, so since $b \in \mathrm{N}_m$, we have

$$|c|_m = \frac{|b|_m}{(|b|_m + 1, |b|_m)} = |b|_m$$

□

Theorem 5.22 *Let $a \in \mathrm{R}_m,\ b \in \mathrm{N}_m$ be such that $|a|_m \mid |b|_m$. Then the following inference holds*

$$\exists \mathrm{ind}^m_a\ b^n \ \Rightarrow\ \exists \mathrm{ind}^m_b\ a^n \quad (n \in \mathbb{N})$$

Proof Let $n \in \mathbb{N}$ be such that $b^n \in_m \langle a\rangle_m$. Then $\exists k \in \mathbb{N}:\ b^n \equiv a^k \pmod m$. From this we have

$$|b^n|_m = |a^k|_m \ \Rightarrow\ (k, |a|_m)\frac{|b|_m}{|a|_m} = (n, |b|_m) \ \Rightarrow\ (k, |a|_m) \mid n$$

So $\exists l \in \mathbb{N}:\ kl \equiv n \ (\mathrm{mod}\ |a|_m)$, which implies $a^n \equiv a^{kl} \equiv b^{nl} \pmod m$. □

It is easy to find numbers $m \in \mathbb{N},\ a, b \in \mathrm{N}_m$ for which the theorem above does not hold.

Theorem 5.23 *Let $a, b \in \mathrm{R}_m$ be such that $|a|_m = |b|_m$. Then the following equivalence holds*

$$b^n \in_m \langle a \rangle_m \ \Leftrightarrow \ a^n \in_m \langle b \rangle_m \quad (n \in \mathbb{N})$$

Proof Follows easily from Theorem 5.22. □

Definition 5.5 *For $a, b \in \mathrm{R}_m$ we will say that a and b are equivalent modulo m if the following are true*

$$a^{|a|_m} \equiv b^{|b|_m} \pmod{m} \text{ and } |a|_m = |b|_m \text{ and } \exists \mathrm{ind}_b^m a$$

and we shall denote it as $a \sim_m b$.

Theorem 5.24 *The relation $\sim_m$ truly is an equivalence relation.*

Proof It is clear that $a \sim_m a$ for all $a \in \mathrm{R}_m$.
By the previous theorem, we have that for all $a, b \in \mathrm{R}_m$

$$a \sim_m b \ \Leftrightarrow \ |a|_m = |b|_m, \ \exists \mathrm{ind}_b^m a \ \Leftrightarrow \ |a|_m = |b|_m, \ \exists \mathrm{ind}_a^m b \ \Leftrightarrow \ b \sim_m a$$

Now, to show the transitivity of our relation, we take any $a, b, c \in \mathrm{R}_m$

$$a \sim_m b, \ b \sim_m c \ \Rightarrow \ |a|_m = |b|_m = |c|_m, \ \exists n, k: \ b^n \equiv a, \ c^k \equiv b \pmod{m} \ \Rightarrow$$

$$\Rightarrow \ |a|_m = |c|_m, \ c^{nk} \equiv a \pmod{m} \ \Rightarrow \ a \sim_m c$$

□

Theorem 5.25 *Let $a, b \in \mathrm{R}_m$, $n \in \mathbb{N}$ be such that $b^n \in_m \langle a \rangle_m$, $(n, |b|_m) = 1$. Then $\langle b \rangle_m \subset \langle a \rangle_m$.*

Proof Let $k \in \mathbb{N}$ be such that $b^n \equiv a^k \pmod{m}$. Let l be any integer. Then $\exists s \in \mathbb{N}:$ $ns \equiv l \pmod{|b|_m}$. From this we have $b^l \equiv a^{ks} \pmod{m}$, which implies $b^l \in_m \langle a \rangle_m$. □

Theorem 5.26 *Let $a, b \in \mathrm{R}_m$, $n \in \mathbb{N}$ be such that $a^n \in_m \langle b \rangle_m$ and $|b|_m \mid |a|_m$, $(n, |b|_m) = 1$. Then $\langle b \rangle_m \subset \langle a \rangle_m$.*

Proof By Theorem 5.22 we have that $b^n \in_m \langle a \rangle_m$, so we have $\langle b \rangle_m \subset \langle a \rangle_m$ by Theorem 5.25. □

Theorem 5.27 *For $a, b \in \mathrm{R}_m$, we have $\langle a \rangle_m = \langle b \rangle_m$ iff $|a|_m = |b|_m$ and there exists some $n \in \mathbb{N}$ such that $(n, |a|_m) = 1$ and $a^n \in_m \langle b \rangle_m$.*

Proof First, let us suppose that $\langle a \rangle_m = \langle b \rangle_m$. Then

$$|a|_m = |\langle a \rangle_m| = |\langle b \rangle_m| = |b|_m$$

Also, for any $n \in \mathbb{N}$, $(n, |a|_m) = 1$, we have $a^n \in_m \langle a \rangle_m = \langle b \rangle_m$.
Now, let us suppose that $|a|_m = |b|_m$ and there exists some $n \in \mathbb{N}$ such that $(n, |a|_m) = 1$ and $a^n \in_m \langle b \rangle_m$. Then by Theorem 5.25, we have that $\langle a \rangle_m \subset \langle b \rangle_m$. By Theorem 5.23, we have that $b^n \in_m \langle a \rangle_m$, so by applying Theorem 5.25 once again, we get $\langle b \rangle_m \subset \langle a \rangle_m$ as well. □

Theorem 5.28 *Let $a, b \in \mathrm{R}_m$ be such that $|a|_m \mid |b|_m$. Then there exists some $c \in \mathrm{R}_m$ such that $a, b \in \langle c\rangle_m$, iff $a \in \langle b\rangle_m$.*

Proof Let us suppose that $a, b \in \langle c\rangle_m$ for some $c \in \mathrm{R}_m$. Then

$$(\mathrm{ind}_c^m b, |c|_m) = \frac{|c|_m}{|b|_m} \mid \frac{|c|_m}{|a|_m} = (\mathrm{ind}_c^m a, |c|_m) \mid \mathrm{ind}_c^m a$$

So there exists some $k \in \mathbb{N}$ such that $(\mathrm{ind}_c^m b)k \equiv \mathrm{ind}_c^m a \pmod{|c|_m}$. So $b^k \equiv a \pmod{m}$. Now, if $a \in \langle b\rangle_m$, then with $c := b$, we have that $a, b \in \langle c\rangle_m$. $\square$

Theorem 5.29 *Let $e \in \mathrm{E}_m$, $a, b \in \mathrm{R}_m^e$ be such that $(|a|_m, |b|_m) = 1$. Then $\langle a\rangle_m \cap \langle b\rangle_m = \{e\}$.*

Proof Let us take $c \in \langle a\rangle_m \cap \langle b\rangle_m$. Then there exists some $n \in \mathbb{N}$ such that $n|b|_m \equiv \mathrm{ind}_a^m c \pmod{|a|_m}$. So we have

$$a^{n|b|_m^2} \equiv a^{|b|_m \mathrm{ind}_a^m c} \equiv c^{|b|_m} \equiv (b^{|b|_m})^{\mathrm{ind}_b^m c} \equiv e \pmod{m} \Rightarrow |a|_m \mid n|b|_m^2 \Rightarrow$$

$$\Rightarrow |a|_m \mid n \Rightarrow \mathrm{ind}_a^m c \equiv n|b|_m \equiv 0 \pmod{|a|_m} \Rightarrow c \equiv a^{\mathrm{ind}_a^m c} \equiv e \pmod{m}$$

$\square$

Theorem 5.30 *For $b \in \mathrm{R}_m$, $a \in \langle b\rangle_m$, $d \mid |b|_m$ the following equivalence holds*

$$|a|_m = d \Leftrightarrow \mathrm{ind}_b^m a = \frac{r|b|_m}{d}, \ (r, d) = 1$$

Proof First, let us suppose that $|a|_m = d$. Then

$$d = |a|_m = \frac{|b|_m}{(\mathrm{ind}_b^m a, |b|_m)} \Rightarrow \mathrm{ind}_b^m a = \frac{r|b|_m}{d}, \ r := \frac{\mathrm{ind}_b^m a}{(\mathrm{ind}_b^m a, |b|_m)}$$

where we see that $(r, |a|_m) = 1$.
Now, let $r, d, b \in \mathbb{N}$ be any numbers such that $(r, d) = 1$, $d \mid b$. Then

$$\frac{b}{(\frac{rb}{d}, b)} = d$$

Considering the relation between prime-factorizations and the greatest common divisor, we need to show that for all $r, d, b \geq 0$, $\min(r, d) = 0$, $d \leq b$, we have $b - \min(r + b - d, b) = d$. Supposing that $r \leq d$, we get $r = 0$, from which the desired relation is $b - (b - d) = d$. Now, if $d \leq r$, then $d = 0$, so the relation we need is $b - b = 0$.
Applying the relation above, we get that

$$|a|_m = \frac{|b|_m}{\left(\frac{r|b|_m}{d}, |b|_m\right)} = d$$

$\square$

Theorem 5.31 *For $a \in \mathrm{R}_m$, $d \mid |a|_m$*

$$|\{b \in \langle a\rangle_m : \ |b|_m = d\}| = \varphi(d)$$

and

$$|\{b \in \mathrm{R}_m : \ b \sim_m a\}| = \varphi(|a|_m)$$

Proof The first equality follows from the above theorem.
The second one follows from the first with $d = |a|_m$. □

We now examine further properties of the function $\mathrm{D}_m(a, b)$.

Definition 5.6 *For $e \in \mathrm{E}_m, \ a, b \in \mathrm{R}_m^e$, let the relative order of the numbers a and b be defined as*

$$|a, b|_m := |\langle a\rangle_m \cap \langle b\rangle_m| = \frac{|a|_m}{\mathrm{D}_m(a, b)} = \frac{|b|_m}{\mathrm{D}_m(b, a)}$$

Theorem 5.32 *For $e \in \mathrm{E}_m, \ a, b \in \mathrm{R}_m^e, \ n \in \mathbb{N}$*

$$\mathrm{D}_m(a, b) = \mathrm{D}_m(b, a) \ \Leftrightarrow \ |a|_m = |b|_m$$

$$\frac{\mathrm{D}_m(a, b)}{\mathrm{D}_m(b, a)} = \frac{|a|_m}{|b|_m}$$

$$\mathrm{D}_m(a, b) = \left| a^{|a^{\mathrm{D}_m(a,b)}|_m} \right|_m$$

$$\mathrm{D}_m(a^n, b) = \frac{\mathrm{D}_m(a, b)}{(n, \mathrm{D}_m(a, b))}$$

$$(|a, b|_m, \mathrm{D}_m(b, a)) = 1 \ \Rightarrow \ \mathrm{D}_m(a, b^n) = \mathrm{D}_m(a, b)\left(n, \frac{|a|_m}{\mathrm{D}_m(a, b)}\right)$$

Proof The first, second, and third relations follow trivially from Theorem 5.17. To prove the fourth relation, for any $k \in \mathbb{N}$ we see that

$$\mathrm{D}_m(a^n, b) \mid k \ \Leftrightarrow \ a^{nk} \in_m \langle b\rangle_m \ \Leftrightarrow \ \mathrm{D}_m(a, b) \mid nk \ \Leftrightarrow \ \frac{\mathrm{D}_m(a, b)}{(n, \mathrm{D}_m(a, b))} \mid k$$

To prove the fifth relation,

$$\mathrm{D}_m(a, b^n) = \frac{|a|_m}{|b^n|_m}\mathrm{D}_m(b^n, a) = \frac{|a|_m}{|b|_m}(n, |b|_m)\frac{\mathrm{D}_m(b, a)}{(n, \mathrm{D}_m(b, a))} =$$

$$= \mathrm{D}_m(a, b)\frac{(n, |b|_m)}{(n, \mathrm{D}_m(b, a))} = \mathrm{D}_m(a, b)\left(n, \frac{|b|_m}{\mathrm{D}_m(b, a)}\right) =$$

$$= \mathrm{D}_m(a, b)\left(n, \frac{|a|_m}{\mathrm{D}_m(a, b)}\right)$$

□

Theorem 5.33 *For $e \in \mathrm{E}_m, \ a, b \in \mathrm{R}_m^e, \ n, k \in \mathbb{N}$*

$$|a, b|_m = |b, a|_m$$

$$|a, a|_m = |a|_m$$

$$(|a|_m, |b|_m) = 1 \ \Rightarrow \ |a, b|_m = 1$$

$$b \in \langle a\rangle_m \;\Rightarrow\; |a,b|_m = |b|_m$$

$$(|a,b|_m, \mathrm{D}_m(a,b)) = 1 \;\Rightarrow\; |a^n,b|_m = \frac{|a,b|_m}{(n,|a,b|_m)}$$

$$(|a,b|_m, \mathrm{D}_m(a,b^k)\mathrm{D}_m(b,a)) = 1 \;\Rightarrow\; |a^n,b^k|_m = \frac{|a,b|_m}{(n(k,|a,b|_m),|a,b|_m)}$$

Proof The first and second relations are trivial.
The first inference follows from Theorem 5.29, and the second is trivial.
Now, to prove the fifth relation,

$$|a^n,b|_m = \frac{|b|_m}{\mathrm{D}_m(b,a^n)} = \frac{|b|_m}{\mathrm{D}_m(b,a)\left(n, \frac{|b|_m}{\mathrm{D}_m(b,a)}\right)} = \frac{|a,b|_m}{(n,|a,b|_m)}$$

Lastly, since

$$(|a,b|_m, D_m(a,b^k)) = 1 \;\Rightarrow\; (|a,b^k|_m, D_m(a,b^k)) = 1$$

we have

$$|a^n,b^k|_m = \frac{|a,b^k|_m}{(n,|a,b^k|_m)} = \frac{|b,a|_m}{(k,|b,a|_m)\left(n, \frac{|b,a|_m}{(k,|b,a|_m)}\right)} = \frac{|a,b|_m}{(n(k,|a,b|_m),|a,b|_m)}$$

□

6 Binomial Congruences

Definition 6.1 *For $a \in \mathbb{Z},\ k \in \mathbb{N}$ let $\mathrm{M}_m(k,a)$ denote the logical function which gives "true" if the equation in x*

$$x^k \equiv a \pmod{m}$$

is solvable, otherwise let its value be "false".
Furthermore, let $\mathrm{S}_m(k,a)$ denote the set of solutions in $\mathbb{Z}_m$ of the equation above, and let $\mathrm{S}_m^{\mathrm{R}}(k,a)$ denote the set of regular solutions in $\mathbb{Z}_m$.
In case of $a \in \mathrm{R}_m$, let $\omega_m(a)$ denote the number

$$\max\left\{|b|_m:\ b \in \mathrm{R}_m,\ \exists \mathrm{ind}_b^m a\right\}$$

furthermore let $\mathrm{ind}^m a := \frac{\omega_m(a)}{|a|_m}$.

Note that $\omega_m(a) = \varphi(m)$ for some $a \in \mathrm{R}_m$, iff R_m^1 is cyclical.

Theorem 6.1 *For $a \in \mathrm{R}_m,\ k \in \mathbb{N}$*

$$\mathrm{M}_m(k,a)\ \Leftrightarrow\ a^{\frac{\omega_m(a)}{(k,\omega_m(a))}} \in_m \mathrm{E}_m$$

Proof Let $b \in \mathrm{R}_m$ be such that $\exists \mathrm{ind}_b^m a$ and $|b|_m = \omega_m(a)$. Then we have

$$a^{\frac{\omega_m(a)}{(k,\omega_m(a))}} \in_m \mathrm{E}_m\ \Leftrightarrow\ (k,|b|_m) \mid \mathrm{ind}_b^m a$$

If $(k,|b|_m) \mid \mathrm{ind}_b^m a$ holds, then there must exist some $1 \le l \le |b|_m$ for which $kl \equiv \mathrm{ind}_b^m a \pmod{|b|_m}$. So we have

$$b^{kl} \equiv b^{\mathrm{ind}_b^m a} \pmod{m}\ \Rightarrow\ (b^l)^k \equiv a \pmod{m}$$

so b^l is a solution of the equation.
Now, let x_0 be a solution of the equation, and denote $e := a^{\varphi(m)} \bmod m,\ \ c := x_0 e \bmod m$. Then we have that c is a solution as well, since

$$c^k \equiv (x_0)^k e \equiv a \cdot a^{|a|_m} \equiv a \pmod{m}$$

and $c \in \mathrm{R}_m$ since

$$c \cdot c^{|c|_m} \equiv c \cdot c^{\varphi(m)} \equiv x_0 e (x_0^k)^{\varphi(m)} \equiv x_0 e \equiv c \pmod{m}$$

It is also clear that $|c|_m \mid |b|_m$. For, let us make the indirect assumption that $|c|_m \nmid |b|_m$. Then we have $|c|_m < |b|_m$ by the definition of $\omega_m(a)$. We also know by Theorem 5.20 that there exists some $d \in \mathrm{R}_m$, such that $\exists \mathrm{ind}_d^m a$ and $|d|_m = [|b|_m, |c|_m]$. It is clear that $|d|_m > |b|_m$, which obviously contradicts the selection of b and the definition of $\omega_m(a)$. So we must have that $|c|_m \mid |b|_m$. From this, we have

$$a^{\frac{\omega_m(a)}{(k,\omega_m(a))}} \equiv a^{\frac{|b|_m}{(k,|b|_m)}} \equiv \left(c^k\right)^{\frac{|b|_m}{(k,|b|_m)}} \equiv \left(c^{|c|_m}\right)^{\frac{|b|_m}{|c|_m}\cdot\frac{k}{(k,|b|_m)}} \equiv e \pmod{m}\ \ \square$$

The difficulty of the verification of the condition

$$a^{\frac{\omega_m(a)}{(k,\omega_m(a))}} \in_m \mathrm{E}_m$$

lies within the calculation of $\omega_m(a)$. So I believe that the examination of the mapping $m \mapsto \omega_m(a)$ is probably the most logical direction, research on this subject should take. Let us look at some immediate corollaries of our theorem.

Theorem 6.2 *For* $a \in \mathrm{R}_m,\ k \in \mathbb{N}$

$$\mathrm{M}_m(k,a) \ \Leftrightarrow\ \mathrm{M}_m((k,\varphi(m)),a) \ \Leftrightarrow\ \mathrm{M}_m((k,\psi(m)),a)$$

Proof The equivalence follows trivially from our previous theorem, since

$$\omega_m(a) \mid \varphi(m), \psi(m) \ \Rightarrow\ (k,\omega_m(a)) = ((k,\varphi(m)),\omega_m(a)) = ((k,\psi(m)),\omega_m(a))$$

□

Theorem 6.3 *For* $a \in \mathrm{R}_m,\ k_1, k_2 \in \mathbb{N}$

$$\mathrm{M}_m(k_1,a) \text{ and } \mathrm{M}_m(k_2,a) \ \Leftrightarrow\ \mathrm{M}_m([k_1,k_2],a)$$

Proof Our theorem follows from Theorem 5.16, and the fact that

$$\left(\frac{\omega_m(a)}{(k_1,\omega_m(a))}, \frac{\omega_m(a)}{(k_2,\omega_m(a))}\right) = \frac{\omega_m(a)}{([k_1,k_2],\omega_m(a))}$$

□

We now look at a necessary and then a sufficient condition for the solvability of a binomial congruence modulo m.

Theorem 6.4 *For* $a \in \mathbb{Z}_m,\ k \in \mathbb{N}$

$$\mathrm{M}_m(k,a) \ \Rightarrow\ a^{\frac{\varphi(m)}{(k,\varphi(m))}} \in_m \mathrm{E}_m$$

Proof Let the solution of the binomial congruence, be denoted by x_0. Then

$$a^{\frac{\varphi(m)}{(k,\varphi(m))}} \equiv (x_0^k)^{\frac{\varphi(m)}{(k,\varphi(m))}} \equiv (x_0^{\varphi(m)})^{\frac{k}{(k,\varphi(m))}} \in_m \mathrm{E}_m$$

□

Theorem 6.5 *Let* $a,b \in \mathrm{R}_m,\ k \in \mathbb{N}$ *be such that* $\exists \mathrm{ind}_b^m a$ *and* $(k,|b|_m) \mid \mathrm{ind}_b^m a$. *Then* $\mathrm{M}_m(k,a)$.

Proof If the conditions above are satisfied, then for some $l \in \mathbb{Z}_{|b|_m}$, we have $kl \equiv \mathrm{ind}_b^m a \pmod{|b|_m}$. So since $b \in \mathrm{R}_m$, we have

$$b^{kl} \equiv b^{\mathrm{ind}_b^m a} \pmod{m} \ \Rightarrow\ b^l \in_m \mathrm{S}_m(k,a) \ \Rightarrow\ \mathrm{M}_m(k,a)$$

□

We now look at some special solutions of a binomial congruence.

Theorem 6.6 *Let* $a, b \in \mathrm{R}_m,\ e \in \mathrm{E}_{|b|_m},\ k, l \in \mathbb{N},\ kl \in \mathrm{R}^e_{|b|_m}$ *be such that* $\exists \mathrm{ind}^m_b a \in \mathrm{R}^e_{|b|_m},\ kl \equiv e \pmod{|b|_m}$ *and* $\mathrm{M}_m(k, a)$*. Then*

$$b^{l\mathrm{ind}^m_b a + n\frac{|b|_m}{(k,|b|_m)}} \in_m \mathrm{S}_m(k, a) \quad (n \in \mathbb{N})$$

Proof

$$k(l\mathrm{ind}^m_b a + n\frac{|b|_m}{(k,|b|_m)}) \equiv \mathrm{ind}^m_b a + n\frac{k}{(k,|b|_m)}|b|_m \equiv \mathrm{ind}^m_b a \pmod{|b|_m} \Rightarrow$$

$$\Rightarrow (b^{l\mathrm{ind}^m_b a + n\frac{|b|_m}{(k,|b|_m)}})^k \equiv b^{\mathrm{ind}^m_b a} \equiv a \pmod{m}$$

□

Next, we examine the number of solutions of a binomial congruence.

Theorem 6.7 *If* $a \in \mathrm{R}_m,\ k \in \mathbb{N}$ *and* $\mathrm{M}_m(k, a)$*, then* $|\mathrm{S}^{\mathrm{R}}_m(k, a)| > 0$*.*

Proof It is clear that $x_0 \cdot e \in_m \mathrm{S}^{\mathrm{R}}_m(k, a)$ for any $x_0 \in \mathrm{S}_m(k, a)$, where $a^{|a|_m} \equiv e \pmod{m}$. □

Theorem 6.8 *If* $e \in \mathrm{E}_m,\ a \in \mathrm{R}^e_m,\ k \in \mathbb{N}$ *and* $\mathrm{M}_m(k, a)$*, then* $|\mathrm{S}^{\mathrm{R}}_m(k, a)| = |\mathrm{S}^{\mathrm{R}}_m(k, e)|$*.*

Proof Let $x_0 \in \mathrm{S}^{\mathrm{R}}_m(k, a)$ be some regular solution. Then according to Theorem 5.13, we have exactly one $x_0^{-1} \in \mathrm{R}^e_m$ such that $x_0^{-1}x_0 \equiv e \pmod{m}$. Let us define the set

$$A := \{x_0^{-1}x_i : \ x_i \in \mathrm{S}^{\mathrm{R}}_m(k, a)\}$$

Then we have that $A \subset \mathrm{S}^{\mathrm{R}}_m(k, e)$, since for any $x_i \in \mathrm{S}^{\mathrm{R}}_m(k, a)$

$$(x_0^{-1}x_i)^k \equiv (x_0^{-1})^k x_i^k \equiv (x_0^{-1})^k x_0^k \equiv e \pmod{m}$$

and for $i \neq j$ we have $x_0^{-1}x_i \not\equiv x_0^{-1}x_j \pmod{m}$, for let suppose that for some $i \neq j$

$$x_0^{-1}x_i \equiv x_0^{-1}x_j \ \Rightarrow \ x_i \equiv x_i x_0^{-1} x_0 \equiv x_j x_0^{-1} x_0 \equiv x_j \pmod{m}$$

which is a contradiction. So we have that $|\mathrm{S}^{\mathrm{R}}_m(k, a)| = |A| \leq |\mathrm{S}^{\mathrm{R}}_m(k, e)|$.
We also have that

$$\mathrm{S}^{\mathrm{R}}_m(k, a) = x_0 \cdot \mathrm{S}^{\mathrm{R}}_m(k, e) \bmod m \subset \mathrm{S}^{\mathrm{R}}_m(k, a)$$

so $|\mathrm{S}^{\mathrm{R}}_m(k, e)| \leq |\mathrm{S}^{\mathrm{R}}_m(k, a)|$. □

7 Generalized Primitive Roots

Definition 7.1 *A number $g \in \mathrm{R}_m$ is said to be a generalized primitive root modulo m, if $\omega_m(g) = |g|_m$. Let the set of such g be denoted by G_m.*
Furthermore, let $\Omega_m(a)$ denote the set

$$\{b \in \mathrm{R}_m : \ \exists \mathrm{ind}_b^m a \text{ and } |b|_m = \omega_m(a)\}$$

Theorem 7.1 *For all $a \in \mathrm{R}_m$*

$$\Omega_m(a) \subset \mathrm{G}_m$$

Furthermore, for all $g \in \mathrm{G}_m$ there exists some $a \in \mathrm{R}_m$ such that $g \in \Omega_m(a)$.

Proof To prove the first part of our theorem, take any $b \in \Omega_m(a)$, and let us suppose indirectly that $b \notin \mathrm{G}_m$. Then there exists some $c \in \mathrm{R}_m$, such that $\exists \mathrm{ind}_c^m b$ and $|c|_m > |b|_m$. Obviously $\exists \mathrm{ind}_c^m a$, since

$$(c^{\mathrm{ind}_c^m b})^{\mathrm{ind}_b^m a} \equiv b^{\mathrm{ind}_b^m a} \equiv a \pmod m$$

Which contradicts the maximality of $|b|_m = \omega_m(a)$.
Now, to prove the second part, take any $g \in \mathrm{G}_m$. It is trivial, that $g \in \Omega_m(g)$. □

Note that our theorem implies the nonemptyness of G_m.

Theorem 7.2 *For $a \in \mathrm{R}_m, \ g \in \Omega_m(a)$ the following equivalence holds*

$$g^n \in_m \Omega_m(a) \ \Leftrightarrow \ (n, |g|_m) = 1 \quad (n \in \mathbb{N})$$

Proof To prove the $\Rightarrow$ part of the equivalence

$$|g|_m = \omega_m(a) = |g^n|_m = \frac{|g|_m}{(n, |g|_m)} \ \Rightarrow \ (n, |g|_m) = 1$$

Now, if we suppose that $(n, |g|_m) = 1$, then there exists some $k \in \mathbb{N}$ such that $nk \equiv \mathrm{ind}_g^m a \pmod{|g|_m}$. So

$$(g^n)^k \equiv g^{\mathrm{ind}_g^m a} \equiv a \pmod m \ \Rightarrow \ \exists \mathrm{ind}_{g^n}^m a$$

and

$$|g^n|_m = \frac{|g|_m}{(n, |g|_m)} = |g|_m = \omega_m(a)$$

So $g^n \in_m \Omega_m(a)$. □

Theorem 7.3 *For $a \in \mathrm{R}_m$ the following equivalence holds*

$$g \in \Omega_m(a) \ \Leftrightarrow \ g^{-1} \in \Omega_m(a)$$

Proof Follows from our previous theorem. □

Theorem 7.4 *Let $m_1, m_2 \in \mathbb{N}$ be such that $m = [m_1, m_2]$, and $g \in \mathbb{Z}_m$. If $g \in_{m_1} \mathrm{G}_{m_1}$ and $g \in_{m_2} \mathrm{G}_{m_2}$, then $g \in_m \mathrm{G}_m$.*

Proof Let us suppose indirectly, that $g \notin \mathrm{G}_m$. This means that there exists some $h \in \mathrm{R}_m$ and $n \in \mathbb{N}$, such that $|h|_m > |g|_m$, and $h^n \equiv g \pmod{m}$. This implies that $(n, |h|_m) > 1$, and for $i \in \{1, 2\}$

$$h^n \equiv g \pmod{m_i} \;\Rightarrow\; |g|_{m_i} = \frac{|h|_{m_i}}{(n, |h|_{m_i})} \;\Rightarrow\; (n, |h|_{m_i}) = 1$$

So combining the two we get

$$1 = [(n, |h|_{m_1}), (n, |h|_{m_2})] = (n, [|h|_{m_1}, |h|_{m_2}]) = (n, |h|_m)$$

which is a contradiction. □

Our theorem above sheds some light on the still hazy structure of G_m.

Theorem 7.5 *If $a, b \in \mathrm{R}_m$, $a \sim_m b$, then $\omega_m(a) = \omega_m(b)$.*

Proof It is clear, that $(\mathrm{ind}_b^m a, |b|_m) = 1$. So for any $g \in \Omega_m(b)$

$$(g^{\mathrm{ind}_g^m b})^{\mathrm{ind}_b^m a} \equiv a \pmod{m}$$

so $\exists \mathrm{ind}_g^m a$. So

$$\omega_m(b) = |g|_m \leq \omega_m(a)$$

The inequality $\omega_m(a) \leq \omega_m(b)$ may be proven in the same way. □

The theorem above shows, that in our quest of finding an easy method for the calculation of the function ω_m, it would be worth examining the equivalence classes according to the relation $\sim_m$. It also implies that if a number is equivalent to a gen. primitive root, then it is a gen. primitive root as well. Therefore, it would also be worth examining the structure of G_m and $\Omega_m(a)$, partitioned according to our equivalence relation.

8 Number Theoretic Functions

In this section, we shall examine some functions, along with some of their properties, emerging from the discussions above.

Definition 8.1 *A number theoretic function $f : \mathbb{N} \to \mathbb{N}$ is said to be multiplicative, if for all $a, b \in \mathcal{D}(f)$, $(a,b) = 1$*

$$a \cdot b \in \mathcal{D}(f) \text{ and } f(a \cdot b) = f(a) \cdot f(b)$$

and we shall denote it as $f \in \mathcal{M}$.
We will say that f is quasimultiplicative, if for all $a, b \in \mathcal{D}(f)$

$$[a,b] \in \mathcal{D}(f) \text{ and } f([a,b]) = [f(a), f(b)]$$

and we shall denote it as $f \in \mathcal{QM}$.
We will say that f is division-invariant, if the following inference holds for all $a, b \in \mathcal{D}(f)$

$$a \mid b \;\Rightarrow\; f(a) \mid f(b)$$

and we shall denote it as $f \in \mathcal{DI}$.
Lastly, we will say that f is prime-power division-invariant, if for all primes q and $\beta, \gamma \in \mathbb{N}$, $\beta \le \gamma$, such that $q^\beta, q^\gamma \in \mathcal{D}(f)$, we have $f(q^\beta) \mid f(q^\gamma)$; and we shall denote it as $f \in \mathcal{DI}_{p^\alpha}$.

Note that the functions ψ (by our theorem below), $m \mapsto |a|_m$ (with domain $\{m \in \mathbb{N} : a \in_m \mathrm{N}_m\}$), $a \mapsto (a,b)$ are quasimultiplicative. We suspect, that for most (if not all) quasimultiplicative functions, there exists some quick algorithm for their computation. The basis of this conjecture is that the well-known Euclidean Algorithm computes the function $a \mapsto (a,b) \in \mathcal{QM}$. Furthermore, it is also possible, that the computation of most multiplicative functions relies heavily on prime-factorization; that is, their computation is mostly equivalent to prime-factorization, in terms of speed.

Theorem 8.1 *For any $g \in \mathcal{DI}_{p^\alpha}$, $\mathcal{D}(g) = \mathbb{N}$ and $n \in \mathbb{N}$, with prime-factorization $n = \prod_{i \in \mathbb{N}} p_i^{\gamma_i}$, define the function f as*

$$f(n) = \operatorname{lcm}(g(p_i^{\gamma_i}) : \; i \in \mathbb{N})$$

Then $f \in \mathcal{QM}$.

Proof Take $a, b \in \mathcal{D}(f)$, with prime-factorizations $a = \prod_{i \in \mathbb{N}} p_i^{\gamma_i}$, $b = \prod_{i \in \mathbb{N}} p_i^{\delta_i}$. Then

$$f([a,b]) = \operatorname{lcm}(g(p_i^{\max(\gamma_i,\delta_i)}) : \; i \in \mathbb{N}) =$$

$$= \operatorname{lcm}([g(p_i^{\min(\gamma_i,\delta_i)}), g(p_i^{\max(\gamma_i,\delta_i)})] : \; i \in \mathbb{N}) =$$

$$= [\operatorname{lcm}(g(p_i^{\gamma_i}) : \; i \in \mathbb{N}), \operatorname{lcm}(g(p_i^{\delta_i}) : \; i \in \mathbb{N})] = [f(a), f(b)]$$

□

It is interesting to ponder the question whether there would exist such a g for all $f \in \mathcal{QM}$.

Theorem 8.2

$$f \in \mathcal{QM} \;\Leftrightarrow\; f \in \mathcal{DI} \text{ and } (a, b \in \mathcal{D}(f),\; (a,b) = 1 \;\Rightarrow\; f(ab) = [f(a), f(b)])$$

Proof First, let us suppose that $f \in \mathcal{QM}$, and take $a, b \in \mathcal{D}(f)$ such that $a \mid b$. Then

$$f(b) = f([a,b]) = [f(a), f(b)] \;\Rightarrow\; f(a) \mid f(b)$$

Now, suppose that the right hand side of the equivalence holds. Let $a, b \in \mathcal{D}(f)$ and $n_i, k_i \in \mathbb{N}$ $(i = 1, 2, 3)$ be such that

$$a = n_1 n_2 n_3,\;\; b = k_1 k_2 k_3,\;\; n_1 \mid k_1,\;\; k_2 \mid n_2$$

$$1 = (n_i, n_j) = (k_i, k_j) = (n_i, k_j) = (n_3, k_3)\;\; (i \neq j)$$

Such decompositions exist, and are easy to find, by looking at the prime factorizations of a and b. So we have $[a, b] = k_1 n_2 n_3 k_3$, and

$$f([a,b]) = [f(k_1), f(n_2), f(n_3), f(k_3)] = [[f(n_1), f(k_1)], [f(k_2), f(n_2)], f(n_3), f(k_3)] =$$

$$= [[f(n_1), f(n_2), f(n_3)], [f(k_1), f(k_2), f(k_3)]] = [f(a), f(b)]$$

□

Theorem 8.3

$$f \in \mathcal{DI} \;\Leftrightarrow\; \forall a, b \in \mathcal{D}(f) :\; [f(a), f(b)] \mid f([a,b])$$

Proof First, let us suppose that $f \in \mathcal{DI}$. For any $a, b \in \mathcal{D}(f)$

$$a, b \mid [a,b] \;\Rightarrow\; f(a), f(b) \mid f([a,b]) \;\Rightarrow\; [f(a), f(b)] \mid f([a,b])$$

Now, suppose that the right hand side property is what holds for f. Then for any $a, b \in \mathcal{D}(f)$

$$a \mid b \;\Rightarrow\; f([a,b]) = f(b) \;\Rightarrow\; [f(a), f(b)] \mid f(b) \;\Rightarrow\; [f(a), f(b)] = f(b) \;\Rightarrow\; f(a) \mid f(b)$$

□

Theorem 8.4 *If $f \in \mathcal{QM}$ is injective, then the following equivalence holds*

$$a \mid b \;\Leftrightarrow\; f(a) \mid f(b)\;\; (a, b \in \mathcal{D}(f))$$

Proof If $f \in \mathcal{QM}$, then by Theorem 8.2, we have the $\Rightarrow$ part of the equivalence.
Now, suppose that $a, b \in \mathcal{D}(f)$ and $f(a) \mid f(b)$. Then

$$f(b) = [f(a), f(b)] = f([a,b]) \;\Rightarrow\; b = [a,b] \;\Rightarrow\; a \mid b$$

□

Definition 8.2 *For $e \in \mathrm{E}_m$, $k \in \mathbb{N}$, let us define the following sets*

$${}_k\mathrm{R}_m := \{a \in \mathrm{R}_m :\; |a|_m = k\},\quad {}_k\mathrm{R}^e_m :=\; {}_k\mathrm{R}_m \cap \mathrm{R}^e_m$$

Now, define

$$r_m^e(k) := |{}_k\mathrm{R}_m^e| \quad (k \in \mathbb{N})$$

Furthermore, let

$$\rho_m^e(k) := |\{a \in \mathrm{R}_m^e : \ |a|_m \mid k\}| \quad (k \in \mathbb{N})$$

Note that by Theorem 6.8 we have that

$$|\mathrm{S}_m^{\mathrm{R}}(k,a)| = |\mathrm{S}_m^{\mathrm{R}}(k,e)| = \rho_m^e(k)$$

if $k \in \mathbb{N}, \ e \in \mathrm{E}_m, \ a \in \mathrm{R}_m^e$ and $\mathrm{M}_m(k,a)$.

Theorem 8.5 *For all* $e \in \mathrm{E}_m$

$$r_m^e(k) = r_{\mu_m(e)}^1(k), \quad \rho_m^e(k) = \rho_{\mu_m(e)}^1(k) \quad (k \in \mathbb{N})$$

Furthermore, if m *is weakly even, then* $r_m^e, \rho_m^e \in \mathcal{M}$.

Proof By the application of Theorem 5.11, we have the first statement of the theorem. So, this result shows that it is enough to prove the multiplicativity of our functions for the case of $e = 1$.
Let $k_1, k_2 \in \mathbb{N}$ be such that $(k_1, k_2) = 1$ and $r_m^1(k_1), r_m^1(k_2) > 0$ (otherwise the theorem holds trivially). Let $k := k_1 k_2$ and $n := \omega(m)$. The following equivalence is quite trivial. For all $x \in \mathbb{N}^n$

$$[x] = k \ \Leftrightarrow \ \exists! u, v \in \mathbb{N}^n : \ x_i = u_i v_i, \ (u_i, v_i) = 1 \ (1 \le i \le n) \text{ and } k_1 = [u], \ k_2 = [v]$$

For simplicity's sake, let us suppose that $\alpha_i > 0$ for all $1 \le i \le n$. Let f denote the integral vector $(\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_n^{\alpha_n}))$.
Since m is weakly even, we know that for all moduli $p_i^{\alpha_i}$ $(1 \le i \le n)$, there exists a primitive root modulo $p_i^{\alpha_i}$. So, it is well-known, that if a primitive root exists modulo $p_i^{\alpha_i}$, then the number of integers in $\mathbb{Z}_{p_i^{\alpha_i}}$ of order $d \in \mathbb{N}$ is $\varphi(d)$ (for $d \mid \varphi(p_i^{\alpha_i})$). Now, with the above facts, and the Chinese Remainder Theorem in mind, we have the following

$$r_m^1(k) = \sum \left(\prod_{i=1}^n \varphi(x_i) : \ x \in \mathbb{N}^n, \ [x] = k, \ x \mid f \right) =$$

$$= \sum \left(\prod_{i=1}^n \varphi(x_i) : \ u \in \mathbb{N}^n, \ [u] = k_1, \ u \mid f, \ v \in \mathbb{N}^n, \ [v] = k_2, \ v \mid f \right) =$$

$$= \sum \left(\left(\prod_{i=1}^n \varphi(u_i) \right) \left(\prod_{i=1}^n \varphi(v_i) \right) : \ u \in \mathbb{N}^n, \ [u] = k_1, \ u \mid f, \ v \in \mathbb{N}^n, \ [v] = k_2, \ v \mid f \right) =$$

$$= \left(\sum \left(\prod_{i=1}^n \varphi(u_i) : \ u \in \mathbb{N}^n, \ [u] = k_1, \ u \mid f \right) \right) \cdot$$

$$\cdot \left(\sum \left(\prod_{j=1}^n \varphi(v_j) : \ v \in \mathbb{N}^n, \ [v] = k_2, \ v \mid f \right) \right) =$$

$$= r_m^1(k_1) \cdot r_m^1(k_2)$$

The multiplicativity of the function ρ^1_m, may be shown similarly. All we need to do, is change some equality signs to division signs, as follows,

$$\rho^1_m(k) = \sum\left(\prod_{i=1}^{n}\varphi(x_i):\ x\in\mathbb{N}^n,\ [x]\mid k,\ x\mid f\right) =$$

$$= \sum\left(\prod_{i=1}^{n}\varphi(x_i):\ u\in\mathbb{N}^n,\ [u]\mid k_1,\ u\mid f,\ v\in\mathbb{N}^n,\ [v]\mid k_2,\ v\mid f\right) =$$

$$= \sum\left(\left(\prod_{i=1}^{n}\varphi(u_i)\right)\left(\prod_{i=1}^{n}\varphi(v_i)\right):\ u\in\mathbb{N}^n,\ [u]\mid k_1,\ u\mid f,\ v\in\mathbb{N}^n,\ [v]\mid k_2,\ v\mid f\right) =$$

$$= \left(\sum\left(\prod_{i=1}^{n}\varphi(u_i):\ u\in\mathbb{N}^n,\ [u]\mid k_1,\ u\mid f\right)\right)\cdot$$

$$\cdot\left(\sum\left(\prod_{j=1}^{n}\varphi(v_j):\ v\in\mathbb{N}^n,\ [v]\mid k_2,\ v\mid f\right)\right) =$$

$$= r^1_m(k_1)\cdot r^1_m(k_2)$$

□

So the theorem above, tells us, that if m is weakly even, then it is enough to determine r^e_m and ρ^e_m at the prime-power divisors of $k\in\mathbb{N}$.

Theorem 8.6 *Supposing that m is weakly even, $\beta\in\mathbb{N}$, $q\in\mathbb{N}$ is prime, $q^\beta\mid\psi(m)$, $n=\omega(m)$, and without hurting generality, we may also suppose that for some $\delta\in(\mathbb{N}\cup\{0\})^n$*

$$\alpha_i>0,\ \varphi(p_i^{\alpha_i})=q^{\delta_i}r_i,\ (q,r_i)=1\quad(1\le i\le n)$$

Then

$$\rho^1_m(q^\beta)=q^{\sum_{i=1}^{n}\min(\beta,\delta_i)}$$

$$r^1_m(q^\beta)=\rho^1_m(q^\beta)-\rho^1_m(q^{\beta-1})$$

$$r^1_m(q)=q^\Delta-1,\quad \Delta=|\{\delta_i\neq 0:\ 1\le i\le n\}|$$

Proof The first relation may be proven in the following manner, by considering the ideas that follow from m being weakly even, like in the proof of the previous theorem,

$$\rho^1_m(q^\beta)=\sum\left(\prod_{i=1}^{n}\varphi(q^{\gamma_i}):\ \max(\gamma)\le\beta,\ \gamma\le\delta\right)=$$

$$=\sum_{\gamma_i\le\min(\beta,\delta_i)} q^{\sum_i\gamma_i}\cdot\left(1-\frac{1}{q}\right)^{\sum_{\gamma_i\neq 0}1}=$$

$$=\prod_{i=1}^{n}\left(1+q\left(1-\frac{1}{q}\right)+q^2\left(1-\frac{1}{q}\right)+\ldots+q^{\min(\beta,\delta_i)}\left(1-\frac{1}{q}\right)\right)=$$

$$= \prod_{i=1}^{n} \left(1 + \frac{q-1}{q}\left(-1 + \frac{q^{\min(\beta,\delta_i)+1} - 1}{q-1}\right)\right) =$$

$$= \prod_{i=1}^{n} \left(1 - 1 + \frac{1}{q} + q^{\min(\beta,\delta_i)} - \frac{1}{q}\right) = q^{\sum_{i=1}^{n} \min(\beta,\delta_i)}$$

The second relation is quite trivial.
The third one follows from the first and the second. □

Theorem 8.7 *If m is weakly even, then*

$$\rho_m^1(k) = \prod_{i=1}^{\infty}(k, \varphi(p_i^{\alpha_i})) \quad (k \in \mathbb{N})$$

Proof First, let us examine the case of $m = p^\alpha$, $\alpha \in \mathbb{N}$, p is prime, and there exists a primitive root modulo p^α, and $k = q^\beta$, q *prime*, $\beta \in \mathbb{N}$.
Then, for some $r \in \mathbb{N}$, we have $\varphi(p^\alpha) = q^\delta r$, $q \nmid r$, so by our previous theorem, we get

$$\rho_{p^\alpha}^1(q^\beta) = q^{\min(\beta,\delta)} = (q^\beta, \varphi(p^\beta))$$

The general case follows quite trivially, through the Chinese Remainder Theorem. □

Theorem 8.8 *If m is weakly even, then $\rho_m^e \in \mathcal{DI}$ for all $e \in \mathrm{E}_m$.*

Proof Follows easily from our previous theorem. □

Theorem 8.9 *For $e \in \mathrm{E}_m$, $k \in \mathbb{N}$*

$$|\langle {}_k\mathrm{R}_m^e \rangle_m| = \frac{k \cdot r_m^e(k)}{\varphi(k)}$$

Proof Let us group the elements of ${}_k\mathrm{R}_m^e$ into equivalence classes, according to the equivalence relation of Definition 5.5. By Theorem 5.31, we have that each equivalence class has $\varphi(k)$ elements, so the number of equivalence classes is $\frac{|{}_k\mathrm{R}_m^e|}{\varphi(k)}$. Each representative of an equivalence class, has an orbit consisting of k elements, so we see that the above relation holds. □

Theorem 8.10 *If m is weakly even, then $k \mapsto |\langle {}_k\mathrm{R}_m^e \rangle_m| \in \mathcal{M}$ for all $e \in \mathrm{E}_m$.*

Proof Our theorem follows easily from Theorem 8.5 and the above relation. □

9 Idempotent Numbers as an Algebraic Structure

Definition 9.1 *For $e, e_1, e_2 \in_m \mathrm{E}_m$, let us define the following operators*

$$\bar{e} := (1 - e) \bmod m$$

$$e_1 \circ e_2 := (e_1 e_2 + \bar{e}_1 \bar{e}_2) \bmod m$$
$$e_1 \otimes e_2 := \overline{\bar{e}_1 \cdot \bar{e}_2}$$
$$e_1 \sim e_2 := \overline{\bar{e}_1 \cdot e_2}$$

Theorem 9.1 *For $e \in \mathrm{E}_m$, $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}$, the following identities hold*

$$(ae + b\bar{e})(ce + d\bar{e}) \equiv (ac)e + (bd)\bar{e} \pmod{m}$$

$$(ae + b\bar{e})^n \equiv (a^n)e + (b^n)\bar{e} \pmod{m}$$

Proof

$$(ae + b\bar{e})(ce + d\bar{e}) \equiv (ac)e + (ad)e\bar{e} + (bc)\bar{e}e + (bd)\bar{e} \equiv (ac)e + (bd)\bar{e} \pmod{m}$$

The second identity follows from the first one. □

Theorem 9.2 *For $e, e_1, e_2 \in \mathrm{E}_m$, we have*

$$\bar{e},\ e_1 \circ e_2,\ e_1 \otimes e_2,\ e_1 \sim e_2 \in \mathrm{E}_m$$

Proof Follows trivially from our previous theorem. □

Definition 9.2 *Let B_m denote the set*

$$\mathrm{B}_m := \{p_i^{\alpha_i} :\ \alpha_i > 0\}$$

For $A \subset \mathrm{B}_m$

$$\bar{A} := \mathrm{B}_m \setminus A$$

For $e \in \mathrm{E}_m$ define

$$\mathrm{B}_m(e) := \{k \in \mathrm{B}_m :\ k \mid e\}$$

Theorem 9.3 *For $e, e_1, e_2 \in \mathrm{E}_m$ the following identities hold*

$$\mathrm{B}_m(\bar{e}) = \overline{\mathrm{B}_m(e)}$$

$$\mathrm{B}_m(e_1 \cdot e_2) = \mathrm{B}_m(e_1) \cup \mathrm{B}_m(e_2)$$
$$\mathrm{B}_m(e_1 \otimes e_2) = \mathrm{B}_m(e_1) \cap \mathrm{B}_m(e_2)$$
$$\mathrm{B}_m(e_1 \sim e_2) = \mathrm{B}_m(e_1) \setminus \mathrm{B}_m(e_2)$$
$$\mathrm{B}_m(e_1 \circ e_2) = \mathrm{B}_m(e_1) \triangle \mathrm{B}_m(e_2)$$

Proof The first two identities are trivial.

$$\mathrm{B}_m(e_1 \otimes e_2) = \mathrm{B}_m(\overline{\bar{e}_1 \cdot \bar{e}_2}) = \overline{\mathrm{B}_m(\bar{e}_1 \cdot \bar{e}_2)} = \overline{\overline{\mathrm{B}_m(e_1)} \cup \overline{\mathrm{B}_m(e_2)}} = \mathrm{B}_m(e_1) \cap \mathrm{B}_m(e_2)$$

$$\mathrm{B}_m(e_1 \sim e_2) = \mathrm{B}_m(e_1) \cap \overline{\mathrm{B}_m(e_2)} = \mathrm{B}_m(e_1) \setminus \mathrm{B}_m(e_2)$$

To prove the last identity, we first make a bit of calculation.

$$(e_1 \sim e_2) \cdot (e_2 \sim e_1) \equiv \overline{\bar{e}_1 e_2} \cdot \overline{e_1 \bar{e}_2} \equiv (1 - \bar{e}_1 e_2)(1 - e_1 \bar{e}_2) \equiv$$

$$\equiv 1 - e_1\bar{e}_2 - \bar{e}_1 e_2 \equiv e_1 + \bar{e}_1 - e_1\bar{e}_2 - \bar{e}_1 e_2 \equiv e_1 \circ e_2 \pmod{m}$$

$$\mathrm{B}_m(e_1 \circ e_2) = \mathrm{B}_m((e_1 \sim e_2) \cdot (e_2 \sim e_1)) = \mathrm{B}_m(e_1 \sim e_2) \cup \mathrm{B}_m(e_2 \sim e_1) =$$

$$= (\mathrm{B}_m(e_1) \setminus \mathrm{B}_m(e_2)) \cup (\mathrm{B}_m(e_2) \setminus \mathrm{B}_m(e_1)) = \mathrm{B}_m(e_1) \triangle \mathrm{B}_m(e_2)$$

□

Considering the properties above, we see that an isomorphism may be defined between E_m and the class of subsets of any finite set, which has $\omega(m)$ elements.

Theorem 9.4 *The structure $\langle \mathrm{E}_m; \{1, ^{-1}, \circ\}\rangle$ is an Abelian group, where each element is of order two.*

Proof First, we will show that for all $e_1, e_2 \in \mathrm{E}_m$, there exists one and only one $e_3 \in \mathrm{E}_m$ such that $e_1 = e_2 \circ e_3$.
Let us take any $e \in \mathrm{E}_m$. Then

$$e_2 \circ e \equiv \bar{e}_2 - (\bar{e}_2 - e_2)e \pmod{m}$$

and $(\bar{e}_2 - e_2, m) = 1$ since $(\bar{e}_2 - e_2)^2 \equiv 1 \pmod{m}$. So by Theorem 3.5 we have

$$|e_2 \circ \mathrm{E}_m| = |\bar{e}_2 - (\bar{e}_2 - e_2)\mathrm{E}_m| = |(\bar{e}_2 - e_2)\mathrm{E}_m| = 2^{\omega\left(\frac{m}{(\bar{e}_2 - e_2, m)}\right)} = 2^{\omega(m)} = |\mathrm{E}_m|$$

which proves both the existence and unicity of e_3.
It is clear that $e \circ 1 = e$ and $e \circ e = 1$, so we have the existence of an inverse, and that each element is of order two. It is also obvious that $\circ$ is commutative. In order to show that $\circ$ is associative, take any $e_1, e_2, e_3 \in \mathrm{E}_m$. Then

$$(e_1 \circ e_2) \circ e_3 \equiv (e_1 e_2 + \bar{e}_1 \bar{e}_2) \circ e_3 \equiv (e_1 e_2 + \bar{e}_1 \bar{e}_2)e_3 + (\bar{e}_1 e_2 + e_1 \bar{e}_2)\bar{e}_3 \equiv$$

$$\equiv e_1 e_2 e_3 + \bar{e}_1 \bar{e}_2 e_3 + \bar{e}_1 e_2 \bar{e}_3 + e_1 \bar{e}_2 \bar{e}_3 \equiv e_1(e_2 e_3 + \bar{e}_2 \bar{e}_3) + \bar{e}_1(\bar{e}_2 e_3 + e_2 \bar{e}_3) \equiv$$

$$\equiv e_1 \circ (e_2 e_3 + \bar{e}_2 \bar{e}_3) \equiv e_1 \circ (e_2 \circ e_3) \pmod{m}$$

□

Theorem 9.5 *The $\otimes$ operator is commutative and associative. Multiplication is distributive with respect to $\otimes$, and $\otimes$ is distributive with respect to $\circ$.*

Proof The commutativity of $\otimes$ is trivial. Now, take any $e_1, e_2, e_3 \in \mathrm{E}_m$.

$$(e_1 \otimes e_2) \otimes e_3 \equiv \overline{\overline{(e_1 \otimes e_2)} \cdot \bar{e}_3} \equiv \overline{\overline{\overline{(\bar{e}_1 \cdot \bar{e}_2)}} \cdot \bar{e}_3} \equiv \overline{\bar{e}_1 \cdot \bar{e}_2 \cdot \bar{e}_3} \pmod{m}$$

which proves the associativity of $\otimes$.
Now, to prove the third property, we calculate

$$e_1 \cdot (e_2 \otimes e_3) \equiv e_1 \cdot \overline{\bar{e}_2 \cdot \bar{e}_3} \equiv e_1(1 - (1 - e_2)(1 - e_3)) \equiv e_1 e_3 + e_1 e_2 - e_1 e_2 e_3 \equiv$$

$$\equiv 1-(1-e_1e_2)(1-e_1e_3) \equiv \overline{\overline{e_1e_2}\cdot\overline{e_1e_3}} \equiv (e_1\cdot e_2)\otimes(e_1\cdot e_3) \pmod{m}$$

The fourth property follows from

$$e_1\otimes(e_2\circ e_3) \equiv \overline{\bar{e}_1\overline{(e_2e_3+\bar{e}_2\bar{e}_3)}} \equiv \overline{\bar{e}_1(e_2\bar{e}_3+\bar{e}_2e_3)} \equiv$$

$$\equiv \overline{\bar{e}_1\bar{e}_3-\bar{e}_1\bar{e}_2\bar{e}_3+\bar{e}_1\bar{e}_2-\bar{e}_1\bar{e}_3\bar{e}_2} \equiv \overline{\overline{\overline{\bar{e}_1\bar{e}_2}\cdot\bar{e}_1\bar{e}_3+\bar{e}_1\bar{e}_2\cdot\overline{\bar{e}_1\bar{e}_3}}} \equiv$$

$$\equiv \overline{\bar{e}_1\bar{e}_2}\cdot\overline{\bar{e}_1\bar{e}_3}+\bar{e}_1\bar{e}_2\cdot\bar{e}_1\bar{e}_3 \equiv (e_1\otimes e_2)\circ(e_1\otimes e_3) \pmod{m}$$

□

Theorem 9.6 *The structure $\langle \mathrm{E}_m; \{\circ,\otimes\}\rangle$ is a commutative ring, with $\circ$ being "addition" and $\otimes$ being "multiplication".*

Proof Follows from our previous two theorems. □

We see that because of the isomorphism that exists between E_m and the subsets of a finite set, the above theorem states the well-known fact from Set Theory, that the subsets of a set form a commutative ring with respect to the operators $\cap$ and $\triangle$.

Theorem 9.7 *For $e, e_1, e_2 \in \mathrm{E}_m$, we have*

$$e\cdot\bar{e}\equiv m,\ \ e+\bar{e}\equiv 1 \pmod{m}$$

$$e\circ 1 = e,\ \ e\circ\bar{e}=m,\ \ e\circ m=\bar{e}$$

$$\overline{e_1\circ e_2}=\bar{e}_1\circ e_2=e_1\circ\bar{e}_2$$

$$e_1\circ e_2\equiv(e_1+\bar{e}_2)(\bar{e}_1+e_2)\equiv(e_1-\bar{e}_2)^2\equiv(\bar{e}_1-e_2)^2 \pmod{m}$$

Proof The fourth line of identities seems a bit nontrivial, so we shall prove it in part below.

$$(e_1+\bar{e}_2)(\bar{e}_1+e_2)\equiv e_1\bar{e}_1+e_1e_2+\bar{e}_2\bar{e}_1+\bar{e}_2e_2\equiv e_1e_2+\bar{e}_2\bar{e}_1 \pmod{m}$$

$$(e_1-\bar{e}_2)^2\equiv e_1-2e_1\bar{e}_2+\bar{e}_2\equiv e_1(1-\bar{e}_2)+\bar{e}_2(1-e_1)\equiv e_1e_2+\bar{e}_2\bar{e}_1 \pmod{m}$$

□

Note that the first and second lines of identities show that $\circ$ behaves somewhat like multiplication. In our upcoming theorems, we will prove properties of $\otimes$ which show that it may behave in a sense both like multiplication and addition.

Theorem 9.8 *For $e, e_1, \ldots, e_n \in \mathrm{E}_m$, we have*

$$e\otimes e=e,\ \ e\otimes 1=1$$

$$(e_1\otimes e_2)-(\bar{e}_1\otimes\bar{e}_2)\equiv e_1\cdot e_2-\bar{e}_1\cdot\bar{e}_2 \pmod{m}$$

$$((e_1\otimes e_2)-(\bar{e}_1\otimes\bar{e}_2))^2\equiv e_1\circ e_2 \pmod{m}$$

$$\overline{\bar{e}_1\otimes\bar{e}_2}\equiv e_1\cdot e_2 \pmod{m}$$

$$\bigotimes_{i=1}^{n} e_i=\overline{\prod_{i=1}^{n}\bar{e}_i}$$

$$e \otimes \bar{e} = 1, \;\; e \otimes 0 = e$$

$$(e_1 \cdot e_2) \otimes (\bar{e}_1 \cdot \bar{e}_2) \equiv e_1 \cdot e_2 + \bar{e}_1 \cdot \bar{e}_2 \equiv e_1 \circ e_2 \pmod{m}$$

Proof The first four lines of properties, are quite trivial. The fifth property may be proven via induction, using the associativity of $\otimes$. The sixth and seventh lines are quite trivial calculations as well. □

Our next theorem shows a peculiar property of $\otimes$, in which it behaves both like addition and multiplication. In fact, the second property sheds light on the double nature of this operator.

Theorem 9.9 *For* $e, e_1, e_2 \in \mathrm{E}_m$*, we have*

$$(e_1 \circ e) \otimes (e_2 \circ e) \equiv (e_1 \otimes e_2)e + (\bar{e}_1 \otimes \bar{e}_2)\bar{e} \pmod{m}$$

$$e_1 \otimes e_2 \equiv e_1 + e_2 - e_1 \cdot e_2 \pmod{m}$$

Proof

$$(e_1 \circ e) \otimes (e_2 \circ e) \equiv 1 - \overline{e_1 \circ e} \cdot \overline{e_2 \circ e} \equiv$$

$$\equiv 1 - (\bar{e}_1 e + e_1 \bar{e})(\bar{e}_2 e + e_2 \bar{e}) \equiv 1 - (\bar{e}_1 \bar{e}_2 e + e_1 e_2 \bar{e}) \equiv$$

$$\equiv e + \bar{e} - (\bar{e}_1 \bar{e}_2 e + e_1 e_2 \bar{e}) \equiv (e_1 \otimes e_2)e + (\bar{e}_1 \otimes \bar{e}_2)\bar{e} \pmod{m}$$

The second property is just simple calculation. □

10 Second-Degree Polynomials

Definition 10.1 *For $k \in \mathbb{Z}$, let $\mathrm{S}_{m,k}$ denote the set of solutions of the equation*

$$x^2 \equiv kx \pmod{m}$$

among the elements of $\mathbb{Z}_m$.

Theorem 10.1 *Let $k \in \mathbb{Z}$ be such that $(k, m) = 1$. Then*

$$\mathrm{S}_{m,k} = k\mathrm{E}_m \bmod m$$

Proof Let $i \in \mathbb{N}$ be such that α_i is positive. Then from

$$x_0^2 \equiv kx_0 \pmod{p_i^{\alpha_i}}$$

it follows that

$$x_0 \equiv 0 \text{ or } x_0 \equiv k \pmod{p_i^{\alpha_i}}$$

Let $e \in \mathrm{E}_m$ be such that $\mu_m(x_0) = \mu_m(e)$. Then for all $i \in \mathbb{N}$ we have $x_0 \equiv ke \pmod{p_i^{\alpha_i}}$, so $x_0 \equiv ke \pmod{m}$. So we may conclude that $\mathrm{S}_{m,k} \subset k\mathrm{E}_m \bmod m$.
Now, we see that $k\mathrm{E}_m \bmod m \subset \mathrm{S}_{m,k}$ as well, since for any $e \in \mathrm{E}_m$, we have

$$(ke)^2 \equiv k(ke) \pmod{m}$$

□

Theorem 10.2 *Let $a, b \in \mathbb{Z}$ be such that $(b - a, m) = 1$. Then for all solutions $r \in \mathbb{Z}_m$ of the equation*

$$(x - a)(x - b) \equiv 0 \pmod{m}$$

there exists a unique $e \in \mathrm{E}_m$, such that

$$r \equiv ae + b\bar{e} \pmod{m}$$

Proof Our equation may be rearranged as

$$(x - a)^2 \equiv (b - a)(x - a) \pmod{m}$$

So since $(b - a, m) = 1$, by our previous theorem we have that for all solutions $r \in \mathbb{Z}$, there exists a unique $e \in \mathrm{E}_m$, such that

$$r - a \equiv (b - a)e \pmod{m}$$

which may be rearranged as

$$r \equiv ae + b\bar{e} \pmod{m}$$

□

Theorem 10.3 *Let m and $a \in \mathbb{Z}$ be such that $(2a, m) = 1$. Then for all solutions $r_1, r_2 \in \mathbb{Z}_m$ of the equation*

$$x^2 \equiv a \pmod{m}$$

there exists a unique $e \in \mathrm{E}_m$*, such that*

$$r_1 \equiv r_2(e - \bar{e}) \pmod{m}$$

Proof With the notation above, we have that our equation is equivalent to the equation

$$(x - r_2)(x - (-r_2)) \equiv 0 \pmod{m}$$

Now, since $r_2^2 \equiv a \pmod{m}$, we have $(r_2, m) = (a, m) = 1$, from which we have $(r_2 - (-r_2), m) = 1$ since $2 \nmid m$, so by our previous theorem, we have that there exists a unique $e \in \mathrm{E}_m$, such that

$$r_1 \equiv r_2 e + (-r_2)\bar{e} \equiv r_2(e - \bar{e}) \pmod{m}$$

□

Theorem 10.4 *Let* m *be an odd number, or four times an odd number. Then for all solutions* $r \in \mathbb{Z}_m$ *of the equation*

$$x^2 \equiv 1 \pmod{m}$$

there exists a unique $e \in \mathrm{E}_m$*, such that*

$$r \equiv e - \bar{e} \pmod{m}$$

Proof The case when m is odd, follows from our previous theorem. Now, if m is four times an odd number, then it is easy to see that

$$\omega\left(\frac{m}{(2, m)}\right) = \omega(m)$$

Our equation is equivalent to the equation

$$(x + 1)^2 \equiv 2(x + 1) \pmod{m}$$

so we see that all elements of $2\mathrm{E}_m - 1$ satisfy this equation, and by Theorem 3.5 we also have that

$$|2\mathrm{E}_m - 1 \bmod m| = 2^{\omega\left(\frac{m}{(2,m)}\right)} = 2^{\omega(m)}$$

which is the number of solutions of our equation if m is four times an odd number, so we have that, for all $r \in \mathbb{Z}_m$ satisfying the equation, there exists a unique $e \in \mathrm{E}_m$, such that

$$r \equiv 2e - 1 \equiv e - \bar{e} \pmod{m}$$

□

Theorem 10.5 *Let* m *be an odd number. Then for all* $e \in \mathrm{E}_m$

$$\mathrm{S}_m^{\mathrm{R}}(2, e) \subset \{e(e_0 - \bar{e}_0) \bmod m : e_0 \in \mathrm{E}_m\}$$

Furthermore, if $e \neq m$*, then for all* $e_0 \in \mathrm{E}_m$ *we have* $e(e_0 - \bar{e}_0) \not\equiv e(\bar{e}_0 - e_0) \pmod{m}$*. Moreover, the following properties are valid*

$$|\mathrm{S}_m^{\mathrm{R}}(2, e)| = 2^{\omega(\mu_m(e))}$$

$$\prod \mathrm{S}^{\mathrm{R}}_m(2,e) \equiv (-1)^{2^{\omega(\mu_m(e))-1}} \cdot e \pmod{m}$$

Proof Take any $i \in \mathbb{N}$ such that $p_i \neq 2$, and $a \in \mathrm{S}^{\mathrm{R}}_m(2,e)$. There are two possible cases. If $a^2 \equiv 0 \pmod{p_i^{\alpha_i}}$, then $a \equiv 0 \pmod{p_i^{\alpha_i}}$, since $a \in \mathrm{R}_{p_i^{\alpha_i}}$. If $a^2 \equiv 1 \pmod{p_i^{\alpha_i}}$, then since $p_i \neq 2$ it follows that $a \equiv \pm 1 \pmod{p_i^{\alpha_i}}$. From these two cases, we have that $a \equiv e(e_0 - \bar{e}_0) \pmod{m}$, for some $e_0 \in \mathrm{E}_m$.
Let us suppose indirectly, that there exists some $e_0 \in \mathrm{E}_m$, such that $e(e_0 - \bar{e}_0) \equiv e(\bar{e}_0 - e_0) \pmod{m}$. Then $2(e_0 - \bar{e}_0)e \equiv 0 \pmod{m}$, from which we have $e \equiv 0 \pmod{m}$, since $(2(e_0 - \bar{e}_0), m) = 1$, because

$$(e_0 - \bar{e}_0)^2 \equiv e_0 + \bar{e}_0 \equiv 1 \pmod{m}$$

So $e = m$, which of course is a contradiction.
To prove the third property, observe that for all $a \in \mathrm{S}^{\mathrm{R}}_m(2,e)$

$$a^2 \equiv e \pmod{m} \;\Leftrightarrow\; a^2 \equiv 1 \pmod{\mu_m(e)} \text{ and } a^2 \equiv 0 \left(\operatorname{mod} \frac{m}{\mu_m(e)}\right)$$

So for all $p_i^{\alpha_i} \in \overline{\mathrm{B}_m(e)}$, we have $a \equiv \pm 1 \pmod{p_i^{\alpha_i}}$. Meanwhile $a \equiv 0 \pmod{\frac{m}{\mu_m(e)}}$, since $a \in \mathrm{R}^e_m$. So by the Chinese Remainder Theorem, and since $\omega(\mu_m(e)) = |\overline{\mathrm{B}_m(e)}|$, we have the formula.
By the first property, with the notation $n := 2^{\omega(\mu_m(e))}$, we have

$$\prod \mathrm{S}^{\mathrm{R}}_m(2,e) \equiv e(e_1 - \bar{e}_1)(e_2 - \bar{e}_2)\dots(e_n - \bar{e}_n) \equiv$$

$$\equiv e \cdot \left[(e_1 - \bar{e}_1)\dots(e_{\frac{n}{2}} - \bar{e}_{\frac{n}{2}})\right] \cdot \left[(\bar{e}_1 - e_1)\dots(\bar{e}_{\frac{n}{2}} - e_{\frac{n}{2}})\right] \equiv$$

$$\equiv e \cdot (-1)^{\frac{n}{2}} \pmod{m}$$

□

Definition 10.2 *For $k \in \mathbb{Z}$, $r \in \mathrm{S}_{m,k}$, $e \in \mathrm{E}_m$ define*

$$\bar{r} := (k - r) \bmod m$$

$$r \circ e := (re + \bar{r}\bar{e}) \bmod m$$

$$r \otimes e := (k - \bar{r}\bar{e}) \bmod m$$

Note that we continue to use the same notations as in the previous section. In order to distinguish between these operators that have been denoted the same way, even though they are different, always refer to the set from which the operands have been taken.

Theorem 10.6 *For $k \in \mathbb{Z}$, $r \in \mathrm{S}_{m,k}$, $e \in \mathrm{E}_m$, we have*

$$\bar{r},\; r \circ e,\; r \otimes e \in \mathrm{S}_{m,k}$$

Proof

$$(k - r)^2 \equiv k^2 - 2kr + r^2 \equiv k^2 - 2kr + kr \equiv k(k - r) \pmod{m}$$

$$(r \circ e)^2 \equiv r^2 e + \bar{r}^2 \bar{e} \equiv (kr)e + (k\bar{r})\bar{e} \equiv k(r \circ e) \pmod{m}$$

$$(r \otimes e)^2 \equiv k^2 - 2k\bar{r}\bar{e} + \bar{r}^2\bar{e} \equiv k(k - \bar{r}\bar{e}) \equiv k(r \otimes e) \pmod{m}$$

□

Theorem 10.7 *Take any $e \in \mathrm{E}_m$ and $k \in \mathbb{Z}$. Then*

$$\mathrm{S}_{m,k} = \mathrm{S}_{m,k} \circ e$$

Proof In order to show the equality of the two sets, it is enough for us to prove that for any $r_1, r_2 \in \mathrm{S}_{m,k},\ r_1 \neq r_2$, we have $r_1 \circ e \neq r_2 \circ e$. For let us suppose indirectly, that there exist some $r_1, r_2 \in \mathrm{S}_{m,k},\ r_1 \neq r_2$, such that $r_1 \circ e = r_2 \circ e$. Then

$$r_1 - r_2 \equiv (e - \bar{e})^2(r_1 - r_2) \equiv (e - \bar{e})((r_1 - r_2)e + (r_2 - r_1)\bar{e}) \equiv$$

$$\equiv (e - \bar{e})((r_1 - r_2)e + (\bar{r}_1 - \bar{r}_2)\bar{e}) \equiv (e - \bar{e})(r_1 \circ e - r_2 \circ e) \equiv 0 \pmod{m}$$

So we arrive at a contradiction. □

Theorem 10.8 *For $k \in \mathbb{Z},\ e, e_1, e_2 \in \mathrm{E}_m,\ r \in \mathrm{S}_{m,k}$ the following properties hold*

$$\overline{r \circ e} = r \circ \bar{e} = \bar{r} \circ e$$

$$(r \circ e_1) \circ e_2 = r \circ (e_1 \circ e_2)$$

Proof

$$\overline{r \circ e} \equiv k - (r \circ e) \equiv ke + k\bar{e} - (re + \bar{r}\bar{e}) \equiv \bar{r}e + r\bar{e} \equiv r \circ \bar{e} \equiv \bar{r} \circ e \pmod{m}$$

$$(r \circ e_1) \circ e_2 \equiv (re_1 + \bar{r}\bar{e}_1) \circ e_2 \equiv (re_1 + \bar{r}\bar{e}_1)e_2 + (\bar{r}e_1 + r\bar{e}_1)\bar{e}_2 \equiv$$

$$\equiv re_1e_2 + \bar{r}\bar{e}_1e_2 + \bar{r}e_1\bar{e}_2 + r\bar{e}_1\bar{e}_2 \equiv r(e_1e_2 + \bar{e}_1\bar{e}_2) + \bar{r}(\bar{e}_1e_2 + e_1\bar{e}_2) \equiv$$

$$\equiv r \circ (e_1 \circ e_2) \pmod{m}$$

□

Note that the second property is somewhat like associativity.

Theorem 10.9 *For $k \in \mathbb{Z},\ (k, m) = 1$ and $r \in \mathrm{S}_{m,k}$, the following equivalence holds*

$$r \circ e_1 = r \circ e_2 \ \Leftrightarrow\ e_1 = e_2 \quad (e_1, e_2 \in \mathrm{E}_m)$$

Proof The $\Leftarrow$ part of the equivalence is trivial.
To prove the $\Rightarrow$ part, first we see that

$$(r - \bar{r})^2 \equiv r^2 - 2r\bar{r} + \bar{r}^2 \equiv kr + k\bar{r} \equiv k^2 \pmod{m}$$

Now, let us suppose that $r \circ e_1 = r \circ e_2$. This means that

$$re_1 + \bar{r}\bar{e}_1 \equiv re_2 + \bar{r}\bar{e}_2 \ \Rightarrow\ \bar{r} + (r - \bar{r})e_1 \equiv \bar{r} + (r - \bar{r})e_2 \pmod{m}$$

First subtracting $\bar{r}$, then squaring both sides, we get

$$k^2e_1 \equiv k^2e_2 \pmod{m}$$

which implies that $e_1 = e_2$, since $(k, m) = 1$. □

Definition 10.3 *For $e \in \mathrm{E}_m,\ r_1, r_2 \in \mathrm{S}_{m,e}$ define*

$$r_1 \circ r_2 := (r_1 r_2 + \bar{r}_1 \bar{r}_2) \bmod m$$

$$r_1 \otimes r_2 := \overline{\bar{r}_1 \cdot \bar{r}_2}$$

Same can be said for these operators, as for those of Definition 10.2.

Theorem 10.10 *For $e \in \mathrm{E}_m,\ r_1, r_2 \in \mathrm{S}_{m,e}$, we have*

$$r_1 \circ r_2,\ r_1 \otimes r_2 \in \mathrm{S}_{m,e}$$

Proof

$$(r_1 \circ r_2)^2 \equiv r_1^2 r_2^2 + \bar{r}_1^2 \bar{r}_2^2 \equiv e(r_1 \circ r_2) \pmod{m}$$

$$(\overline{\bar{r}_1 \cdot \bar{r}_2})^2 \equiv e - 2e\bar{r}_1\bar{r}_2 + \bar{r}_1^2\bar{r}_2^2 \equiv e(1 - \bar{r}_1\bar{r}_2) \equiv e(r_1 \otimes r_2) \pmod{m}$$

□

Theorem 10.11 *For $e \in \mathrm{E}_m,\ a, b \in \mathrm{R}_m^e,\ c, d \in \mathbb{Z},\ n \in \mathbb{N},\ r \in \mathrm{S}_{m,e}$, we have*

$$(ar + b\bar{r})(cr + d\bar{r}) \equiv (ac)r + (bd)\bar{r} \pmod{m}$$

$$(ar + b\bar{r})^n \equiv a^n r + b^n \bar{r} \pmod{m}$$

Proof

$$r\bar{r} \equiv 0 \ \Rightarrow\ (ar + b\bar{r})(cr + d\bar{r}) \equiv (ac)r^2 + (bd)\bar{r}^2 \equiv (ea)cr + (eb)d\bar{r} \pmod{m}$$

The second property follows from the first one via induction. □

Theorem 10.12 *For all $e \in \mathrm{E}_m,\ k \in \mathrm{R}_m^e$ we have*

$$\mathrm{S}_{m,k} \cap \mathrm{R}_m^e = \{k\}$$

Proof For any $r \in \mathrm{S}_{m,k} \cap \mathrm{R}_m^e$ we have

$$r \in_{\mu_m(e)} \mathrm{S}_{\mu_m(e),k} \cap \mathrm{R}^1_{\mu_m(e)} = (k\mathrm{E}_{\mu_m(e)} \bmod \mu_m(e)) \cap \mathrm{R}^1_{\mu_m(e)} =$$

$$= \{k \bmod \mu_m(e)\} \ \Rightarrow\ r \equiv k \pmod{\mu_m(e)}$$

So, since

$$r \equiv 0 \equiv k \ \left(\bmod \frac{m}{\mu_m(e)}\right)$$

and $\mu_m(e) = \mu_m(k) = \mu_m(r)$, we have that $r = k$. □

Acknowledgements

I would like to express my vast gratitude to Professor Mihály Szalay, for the enormous amount of time and effort it took to review my paper. Besides his various helpful comments and corrections, I would like to say special thanks to him for his help on the proof of Theorem 5.20, which was a lemma of utmost importance.

References

[1] Andrews G.E., *Number Theory*, Dover Publications Inc., New York, 1994, pp. 49-138.