International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue II February 2018- Available at www.ijraset.com

Idempotents of the Ring $Z_{P^aq^br^c}$ for Distinct Primesp, q, r having Positive Integer as Exponent

Gaurav Mittal[1], Himanshu Singla[2]
[1]*IitRoorkee, Roorkee, india*
[2] *Post Graduate Govt. College, Sector 11, Chandigarh, India*

Abstract: ***The main purpose of this paper is to explicitly find out the non trivial idempotents of the ring*** $Z_{P^aq^br^c}$ ***for distinct primes p, q and r where a, b and c are positive integers.***
Keywords: Idempotent, Euler's Theorem, Chinese Remainder Theorem,

I. INTRODUCTION

Idempotents in rings play an important role in study of rings and modules. Several classes of elements can be defined using idempotents and units, for example clean elements (the elements which can be written as sum of idempotent and a unit), Strongly clean elements (elements which can be written as sum of an idempotent and a unit that commute).Because of their importance , researchers put great efforts to compute idempotents of rings. Important contributions have been made in special cases .Idempotents of ring R have an important connection to decomposition of R modules. These are those special elements of a ring which do not change on multiplying with themselves. An idempotent is a is called non trivial if $a \neq 0, a \neq 1$. For the ring $Z_{p^aq^b}$ where p and q are distinct odd prime numbers, a and b are positive integers, Kanwar et al. in [1, proposition 2.8] found all the idempotents. In this article we find the idempotents of $Z_{P^aq^br^c}$ (Ring of integers modulo $P^aq^br^c$) for distinct primes p, q and r where a,b and c are positive integers. For this we use standard properties of congruence's and Euler's theorem.

II. PRELIMINARIES

Theorem 2.1 For the ring Z_n, where n is a positive integer, total number of idempotents are 2^m, where m is the number of distinct prime divisors of n.
Proof. Let $n = \prod_{i=1}^{m} p_i^{n_i}$ be the prime factorization of n and let $R_i = Z/p_i^{n_i}Z$.
By the Chinese Remainder Theorem we have

$$Z_n \cong R_1 \times R_2 \times \ldots \times R_m \qquad (1)$$

We claim that if p *is a prime number* and $t > 0$ is an integer, then the only idempotents of Z/p^tZ are 0 and 1, i.e., we want to show that, modulop^t the equation

$$x^2 \equiv x \ (mod\ p^t)$$

has only two trivial solutions. Suppose that $x \neq 0$ is a solution of $x^2 \equiv x \ (mod\ p^t)$. We will show that $x \equiv 1 \ (mod\ p^t)$. Clearly, we must have $x = p^r s$ *where* $0 \leq r < t$ and gcd(s,p)=1. Then $s(p^r s - 1) \equiv 0\, mod(p^{t-r})$ which gives us $p^r s \equiv 1 \ (mod(p^{t-r}))$. This is not possible. So r=0 and hence$x = s \equiv 1$ mod(p^t). Thus claim holds and further from (1) it is very clear that the number of idempotents in this ring is2^m.
Corollary 2.1 The ring $Z_{P^aq^br^c}$ where p,q,r are distinct primes and a, b, c are positive integers has 8 idempotents.
Proof. Since the number of distinct prime divisors of $p^aq^br^c$ are 3, i.e. p, q and r. So now by theorem 2.1 result holds.
Theorem 2.2 Euler's theorem: If a and m are positive integers having g.c.d. equal to 1, i.e. (a,m)=1, then $a^{\varphi(m)} \equiv 1 \ (mod\ m)$, where φ is Euler's toteint function.
Proof. For proof of this result and more on Euler's toteint function cf.[3,chapter 7]

III. IDEMPOTENTS OF THE RING $Z_{P^aq^br^c}$ FOR DISTINCT PRIMES P, Q, R

The reom 3.1 Let p,q,r be the distinct primes and a,b,c are positive integers. Then all the idempotents of the ring $Z_{P^aq^br^c}$ modulo $p^aq^br^c$ are given by

©IJRASET (UGC Approved Journal): All Rights are Reserved

$0,1, (p^a q^b)^{ur^{(c-1)}(r-1)}, (p^a r^c)^{vq^{(b-1)}(q-1)}, (q^b r^c)^{wp^{(a-1)}(p-1)},$

$(p^a)^{\left(d\left(q^{(b-1)}r^{(c-1)}(q-1)(r-1)\right)\right)}, (q^b)^{\left(e\left(p^{(a-1)}r^{(c-1)}(p-1)(r-1)\right)\right)}, (r^c)^{\left(f\left(p^{(a-1)}q^{(b-1)}(p-1)(q-1)\right)\right)}$

Where u, v, w, d, e, f are the smallest positive integers such that$ur^{(c-1)}(r-1)-1>0$, $vq^{(b-1)}(q-1)-1>0$, $wp^{(a-1)}(p-1)-1>0$,$d\left(q^{(b-1)}r^{(c-1)}(q-1)(r-1)\right)-1>0$, $e\left(p^{(a-1)}r^{(c-1)}(p-1)(r-1)\right)-1>0$, $f\left(p^{(a-1)}q^{(b-1)}(p-1)(q-1)\right)-1>0$ respectively.

Proof. Let y be an idempotent. So by definition $y^2 \equiv y\ (mod\ p^a q^b r^c)$. Since p,q,r are distinct primes, for solving congruences, we need to solve the system of congruences

$$y^2 \equiv y\ mod(p^a),\ y^2 \equiv y\ mod(q^b),\qquad y^2 \equiv y\ mod(r^c)$$

Now, for the first congruent p^a divides $y^2 - y$ and p being a prime means p^aeither divide y or (y-1). Same thing holds for other two congruences. So each of these three congruences has 2 solutions which are given by y=0 and y=1. Hence, we consider all the possibilities in 4 cases below and from these possibilities, we get 8 idempotents modulo $p^a q^b r^c$.

Case-1.If $y \equiv 0\ (mod\ p^a),\ y \equiv 0\ (mod\ q^b),\ y \equiv 0\ (mod\ r^c)$. Here clearly $y \equiv 0\ mod(p^a q^b r^c)$ as $p^a,\ q^b\ and\ r^c$ divides y and gcd(p^a, q^b, r^c)=1.

Case-2. . If $y \equiv 1\ (mod\ p^a),\ y \equiv 1(mod\ q^b),\ y \equiv 1\ (mod\ r^c)$. Here clearly $y \equiv 1\ mod(p^a q^b r^c)$ as $p^a,\ q^b\ and\ r^c$ divides (y-1) and gcd(p^a, q^b, r^c)=1.

Case-3.If $\equiv 0\ (mod\ p^a),\ y \equiv 0\ (mod\ q^b),\ y \equiv 1\ (mod\ r^c)$. Then,clearly $y \equiv 0\ mod(p^a q^b)$ and $y \equiv 1\ mod(r^c)$. First congruence $y \equiv 0\ mod(p^a q^b)$ implies $y = p^a q^b G$ for some $G \in Z$. On substituting this value in $y \equiv 1\ (mod\ r^c)$, we get $p^a q^b G \equiv 1\ (modr^c)$. From Euler's Theorem

$$(p^a q^b)^{\varphi(r^c)} = (p^a q^b)^{r^{c-1}(r-1)} \equiv 1\ (mod\ r^c)$$

$$(p^a q^b)(p^a q^b)^{ur^{(c-1)}(r-1)-1} \equiv 1\ (mod\ r^c)$$

Where u is the smallest positive integer such that that $ur^{(c-1)}(r-1)-1>0$ and φ is Euler's function. Also as $p^a q^b G \equiv 1\ (modr^c)$, we have$G \equiv (p^a q^b)^{ur^{(c-1)}(r-1)-1}\ (mod\ r^c)$. Thus, we get

$$y \equiv (p^a q^b)^{ur^{(c-1)}(r-1)}(mod\ p^a q^b r^c).$$

For the cases $y \equiv 0\ (mod\ p^a),\ y \equiv 1(mod\ q^b) and\ y \equiv 0\ (mod\ r^c)$and $y \equiv 1\ (mod\ p^a),\ y \equiv 0\ (mod\ q^b),\ y \equiv 0\ (mod\ r^c)$, we can similarly show that $y \equiv (p^a r^c)^{vq^{(b-1)}(q-1)}(mod\ p^a q^b r^c)$ and $y \equiv (q^b r^c)^{wp^{(a-1)}(p-1)}(mod\ p^a q^b r^c)$ respectively where v,w are the smallest positive integers such that $vq^{(b-1)}(q-1)-1>0, wp^{(a-1)}(p-1)-1>0.$

Case-4. If $y \equiv 0\ (mod\ p^a),\ y \equiv 1(mod\ q^b),\ y \equiv 1\ (mod\ r^c)$. Then clearly $y \equiv 1\ mod(q^b r^c)$ also

$y \equiv 0\ (mod\ p^a)$implies$y = p^a G$for some $G \in Z$. On substituting this in $y \equiv 1\ mod(q^b r^c)$, we get $p^a G \equiv 1(mod\ q^b r^c)$. From Euler's Theorem

( ) ( ) = ( ) $^{(-1)\ (-1)(-1)(-1)} \equiv 1$ ( ).

( )( ) $^{(\ (-1)\ (-1)(-1)(-1))-1)} \equiv 1$ ( ).

Where d is smallest positive integer such that $\left(\ (-1)\ (-1)(-1)(-1)\right)-1>0$and is Euler's function. Thus, we get

$\equiv$ ( ) $^{\left(\ (-1)\ (-1)(-1)(-1)\right)-1)}$( ) and in the end

$\equiv$ ( ) $^{\left(\ (-1)\ (-1)(-1)(-1)\right)}$ ( ).

©IJRASET (UGC Approved Journal): All Rights are Reserved

For the cases $\equiv 1$ ( ), $\equiv 1$( ), $\equiv 0$ ( ) and $\equiv 1$ ( ), $\equiv 0$ ( ), $\equiv 1$ ( ), we can similarly prove that $\equiv$ ( ) $\left(\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) \right)$ ( )and $\equiv$ ( ) $\left(\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) \right)$ ( ) respectively where y,z are the smallest positive integers such that $\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) - 1 > 0$, $\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) - 1 > 0$.Thus we get 8 idempotents in all.

Example: Find all the idempotents of $= /315 \cong {}_{3^2} \times {}_5 \times {}_7$.

This ring has 8 idempotents, two of them being 0,1 mod(315). Using same notations as used in above theorem, we have

$= 3$, $= 5$, $= 7$, $= 2$, $= 1$,

$= 1$ $= = = = = = 1$

From theorem one idempotent is given by $\equiv$ ( ) $\left(\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) \right)$ ( ) .Putting all values we get,

$\equiv 3^{2(5^0 7^0 (5-1)(7-1))}$(315)

$\equiv 36$(315)

Similarly $\equiv$ ( ) $\left(\left({}^{(-1)} {}^{(-1)}(-1)(-1) \right) \right)$ ( ). Putting all values we get

$\equiv 5^{(3^1 7^0 (2)(6))}$(315)

$\equiv 190$(315)

Similarly we can find other idempotents by putting the values in the formula.

REFERENCES

[1] PramodKanwar, MeenuKhatkar and R.K. Sharma, Idempotents and units of matrix rings over polynomial rings, International Electronic Journal of Algebra Volume 22 (2017) 147-169
[2] Joseph A. Gallian, Contemporary Abstract Algebra, 8th edition, Thomson Brooks/Cole,2012
[3] David M. Burton, Elementary number theory, 6th edition, McGraw hill publication 2007.

©IJRASET (UGC Approved Journal): All Rights are Reserved