ANALYSIS OF EACH INTEGER AS SUM OF TWO CUBES IN A FINITE INTEGRAL DOMAIN

by SAHIB SINGH, *Department of Mathematics, Clarion State College, Clarion, Pennsylvania 16214, U S.A.*

(Communicated by S. Chowla, F.N.A.)

(*Received* 18 *January* 1973)

In this paper it has been shown that except for 2 elements in each of $GF(2^2)$ and $GF(7)$, all other elements in a finite integral domain are sum of two cubes.

§ 1. It is well known that a finite integral domain is $GF(p^n)$ where p is prime and $n \geqslant 1$. The multiplicative cyclic group of non-zero elements in $GF(p^n)$ will be denoted by $GF^*(p^n)$. Since $GF(p^n)$ is a simple extension of $GF(p)$, therefore using the property of cyclic groups it follows that the members of $GF^*(p)$ form a unique subgroup of $(p-1)$ elements in $GF^*(p^n)$.

Definitions 1—A non-zero cubic residue in $GF(p^n)$ is defined as a member of $GF^*(p^n)$ which is a cubic power of a generator of $GF^*(p^n)$. This is in conformity with the usual definition of a non-zero cubic residue modulo p which is always a cubic power of a primitive root modulo p in $GF(p)$.

Remark: In the following two cases each member of $GF^*(p^n)$ is a cubic residue:

(i) $p=3$ and $n \geqq 1$; (ii) $p \equiv 2 \pmod 3$ and n odd.

These results are based on the fact that a generator λ of $GF^*(p^n)$ is a cubic power of λ. In (i) $\lambda^{3^n} = \lambda$. In (ii) $\lambda^{(p^n-1)} = 1$ which implies that $\lambda^{(2p^n-1)} = \lambda$ and since by hypothesis of (ii) $2p^n - 1 \equiv 0 \pmod 3$, the proof is complete. As a consequence, we will exclude these values of p and n mentioned in (i) and (ii) in our further discussion.

§ 2. For the values of p and n under consideration, we observe that the members of $GF^*(p^n)$ can be partitioned into 3 cosets with the help of the subgroup (called G) of cubic residues in $GF^*(p^n)$. In the sequel we will call these 3 cosets as G, λG and $\lambda^2 G$, where λ, as before, will always be assumed to be a generator of $GF^*(p^n)$. If ω is an imaginary cube root of unity, then the cubic character ψ for members of $GF(p^n)$ would be defined as under:

$\psi(\alpha)=1$ if α is an element of G
$=\omega$ if α belongs to λG
$=\omega^2$ if α belongs to $\lambda^2 G$
$=$zero if α is zero.

§ 3. Two elements β and $\beta+1$ in $GF(p^n)$ would be called consecutive, when none of these is zero. We will call $(\beta+1)$ as successor of β.

A general member of $GF(p^n)$ can be written as $a_0+a_1\theta+\ldots+a_{n-1}\theta^{n-1}$, where θ is a root of some irreducible polynomial of degree n over $GF(p)$. It is easy to see that the members of $GF^*(p^n)-GF^*(p)$ can be divided into $p^{n-1}-1$ classes with p members in each class so that two consecutive members appearing in $GF^*(p^n)-GF^*(p)$ always belong to the same class. After the preliminary spade work, we prove three Lemmas before the discussion of main theorem.

Lemma 1—A member of λG can be decomposed as sum of two cubes if and only if there exist two consecutive members t, $t+1$ with $\psi(t)=1$ and $\psi(t+1)=\omega$.

PROOF: Let two consecutive members stated above exist and β be an arbitrary member of λG, then since the elements considered are in a field therefore the decomposition of β as sum of two cubes can be written as $\beta=\frac{\beta}{t+1}+\frac{\beta t}{t+1}$.

Conversely: If β is an element of λG such that $\beta=\alpha+\alpha_1$ where α and α_1 are both cubic residues, then $\frac{\beta}{\alpha}=1+\frac{\alpha_1}{\alpha}$ which establishes the existence of a consecutive pair $\left(\frac{\alpha_1}{\alpha},\ \frac{\alpha_1}{\alpha}+1\right)$ with $\psi\left(\frac{\alpha_1}{\alpha}\right)=1$ and $\psi\left(\frac{\alpha_1}{\alpha}+1\right)=\omega$. This completes the proof. Since -1 is always a cubic residue, therefore the result of this Lemma will hold if we have the existence of two consecutive members with the cubic character value of one number as 1 and of other as ω without consideration of their order of occurrence. Exactly by the same reasoning it is easy to conclude the following:

Lemma 2—A member of $\lambda^2 G$ can be expressed as sum of two cubes if and only if there exist two consecutive members such that the cubic character value of one member is 1 and of other is ω^2.

Lemma 3—If there exist three members δ, $\delta+1$, $\delta+2$ of $GF^*(p^n)$ such that δ and $\delta+2$ are cubic residues and $\delta+1$ is not a cubic residue, then each member of λG and $\lambda^2 G$ can be decomposed as sum of two cubes.

PROOF: Let the three members referred to above exist. Without loss of generality, we can write $\psi(\delta+1)=\omega$ whereas $\psi(\delta)=\psi(\delta+2)=1$. By Lemma 1, it follows that each member of λG can be expressed as sum of two cubes. Also under this hypothesis $\psi(\delta+1)^2=\omega^2$ and $\psi(\delta^2+2\delta)=1$. Since $(\delta^2+2\delta)$ and $(\delta+1)^2$ are consecutive, the application of Lemma 2 completes the proof.

Main Theorem—Each integer in $GF(p^n)$, trivial representation being allowed, can be expressed as sum of two cubes. There are two members in each of $GF^*(2^2)$ and $GF^*(7)$ which cannot be so decomposed.

PROOF: If λ is a generator of $GF^*(2^2)$, then the members of $GF^*(2^2)$ are λ, $\lambda+1$, 1 and precisely one member belongs to each coset. In this case, the two non-cubic residues λ and $\lambda+1$ cannot be decomposed as sum of cubes. In case of $GF^*(7)$, 1 and 6 are cubic residues, 2 and 5 can be expressed as sum of 2 cubes each, but for 3 and 4 the decompositions require 3 cubes each, namely, $3=1+1+1$ and $4=6+6+6$. Except for these cases, we will now show that each integer in other cases is sum of 2 cubes. In view of the previous remarks it suffices to consider the following cases:

(A) $p\equiv 1 \pmod 3$ and $n\geqslant 1$ is such that 3 does not divide n. In this case $\lambda^{\left(\frac{p^n-1}{p-1}\right)}$ is a primitive root modulo p, where λ is a generator of $GF^*(p^n)$. Since $\left(\frac{p^n-1}{p-1}\right)\not\equiv 0 \pmod 3$, therefore this primitive root mod p is not a cubic residue in $GF(p^n)$. We thus conclude that only those members of $GF^*(p)$ are cubic residues in $GF^*(p^n)$ which are cubic residues modulo p. The decomposition of each non-residue as sum of two cubic residues is linked with the existence of certain consecutive elements mentioned in the above Lemmas. This existence part of these desired consecutive elements for our purpose can be established from the members of $GF^*(p)$ and as a consequence the decomposition follows. The details are as under:

(i) If $\psi(2)=1$, $\psi(3)\neq 1$, then 2, 3, 4 are the required consecutive members mentioned in Lemma 3. The required decomposition is immediate:

(ii) $\psi(2)\neq 1$, $\psi(3)=1$, then again the application of Lemma 3 yields the result because of the existence of 3 consecutive integers, 1, 2 and 3 with $\psi(1)=\psi(3)=1$ and $\psi(2)\neq 1$.

(iii) $\psi(2)=1$, $\psi(3)=1$ and if $\psi(5)\neq 1$, then the consecutive elements 4, 5 and 6 enable us to decompose each non-cubic residue as sum of two cubes. If $\psi(5)=1$, then we continue and look for the occurrence of the first non-cubic residue which would be a prime number say b, then $(b-1)$ and $(b+1)$ are composite and as a consequence $\psi(b-1)=\psi(b+1)=1$ and thus the 3 consecutive members $b-1$, b and $(b+1)$ would be available for proving the desired result.

(iv) $\psi(2)=\omega$, $\psi(3)=\omega$, then using Lemmas 1 and 2 it follows that the consecutive members 1, 2 will split each member of λG as sum of 2 cubes and the consecutive members 8, 9 will take care of members of $\lambda^2 G$.

(v) $\psi(2)=\omega$, $\psi(3)=\omega^2$, and $\psi(7)\neq 1$, then Lemma 3 can be applied on the basis of three consecutive elements 6, 7 and 8.

(vi) $\psi(2)=\omega$, $\psi(3)=\omega^2$ and $\psi(7)=1$, then the pairs (1, 2) and (27, 28) respectively decompose each member of λG and $\lambda^2 G$ as sum of 2 cubes.

This exhausts all cases because the above values recur when we take $\psi(2)=\omega^2$. In view of this, we conclude that when $p > 28$, each non-cubic residue of $GF(p^n)$ can be expressed as sum of 2 cubes. The only primes of this family which remain to be considered are 7, 13 and 19. Leaving 7, which will be discussed in detail later, it can be seen that the pairs (1, 2) and (8, 9) satisfy the conditions of Lemmas 1 and 2 and therefore can be used for the required decomposition in both cases when $p=13$ and $p=19$.

Among the remaining cases when p is odd, each member of $GF^*(p)$ in the following cases is a cubic residue in $GF(p^n)$.

(B) (i) $p\equiv 2 \pmod 3$ and n is even (case of n being odd has been considered),
(ii) $p\equiv 1 \pmod 3$ and 3 divides n.

The above assertion is justified because $\left(\frac{p^n-1}{p-1}\right) \equiv 0 \pmod 3$ and as a consequence the primitive root modulo p namely $\lambda^{\left(\frac{p^n-1}{p-1}\right)}$ is a cubic residue. In these cases, each non-cubic residue can be split as sum of two cubes because of the following observations:

As stated earlier, the members of $GF^*(p^n)-GF^*(p)$ are divided into $p^{n-1}-1$ classes with p members in each class, from consecutive point of view. Since there are $\frac{p^n-1}{3}-(p-1)$ cubic residues in $GF^*(p^n)-GF^*(p)$, therefore it follows that all the cubic residues in $GF^*(p^n)-GF^*(p)$ cannot be accommodated in complete classes. As a consequence, there exists a class in which a cubic residue and a non-cubic residue would appear as consecutive. Since -1 is a cubic residue, it can be inferred that there exist members $\alpha, \alpha+1$ in $GF^*(p^n)-GF^*(p)$ such that $\psi(\alpha)=1$, $\psi(\alpha+1)=\omega$. This enables us to decompose each member of λG as sum of two cubes. For the values of p and n under consideration, it follows that $\frac{p^n-1}{3} > (p^{n-1}-1)$ which means that there exists at least one of $p^{n-1}-1$ classes in which there are two members of λG. Let us suppose that the two members in the same class are β and $\beta+t$ where t belongs to $GF^*(p)$ so that $\psi(\beta)=\psi(\beta+t)=\omega$.

There exists t' in $GF^*(p)$ such that $tt'=1$.

As $\psi(t')=1$, it follows that $\psi(\beta t')=\psi(\beta t'+1)=\omega$.

This means that $\psi\left(\frac{1}{\beta t'}\right)=\omega^2$ and $\psi\left(1+\frac{1}{\beta t'}\right)=1$.

Thus the condition of Lemma 2 is satisfied and as a consequence, each member of $\lambda^2 G$ can be expressed as sum of two cubes.

(C) Now we consider the case when $p=2$ and $n>2$. Here, by same argument as in case of $p\equiv 2 \pmod 3$, it follows that when n is odd, all the members of $GF^*(2^n)$ are cubic residues. Hence we examine the case when n is even. Since $n=2$ has been discussed therefore we have $n\geqslant 4$. In this case, there are $2^{n-1}-1$ classes in $GF^*(2^n)-GF^*(2)$ with two members in each class, which are consecutive to each other. If there exist two consecutive members α, $\alpha+1$ such that $\psi(\alpha)=1$ and $\psi(\alpha+1)=\omega$, then the decomposition of each member of λG as sum of two cubes is available. Also in that case $\psi(\alpha^2)=1$ and $\psi(\alpha^2+1)=\psi(\alpha+1)^2=\omega^2$ and this takes care of members of $\lambda^2 G$ as well. In case there exist 2 consecutive members β, $\beta+1$ such that $\psi(\beta)=\omega=\psi(\beta+1)$, then $\psi\left(\frac{1}{\beta}\right)=\omega^2$ and $\psi\left(1+\frac{1}{\beta}\right)=1$ Similarly $\psi\left(\frac{1}{\beta^2}\right)=\omega$ and $\psi\left(1+\frac{1}{\beta}\right)^2=1$. Thus by above reasoning, the conclusion follows.

It will be shown that all the cubic residues in $GF^*(2^n)-GF^*(2)$ occupying complete classes and each remaining class having one member of λG and other of $\lambda^2 G$ is not possible. If this hypothesis were true, then we have $\psi(\lambda)=\omega$ and $\psi(\lambda+1)=\omega^2$, where λ is a generator of $GF^*(2^n)$. This means that $\psi(\lambda^2+\lambda)=1$ which in turn implies that $\psi(\lambda^2+\lambda+1)=1$. Now $\psi\ \lambda^3)=1$ and as a consequence $\psi(\lambda^3+1)=1$ # But $\psi(\lambda^3+1)=\psi(\lambda+1)$ $\psi(\lambda^2-\lambda+1)=\psi(\lambda+1)$ $\psi(\lambda^2+\lambda+1)=\omega^2$ which contradicts #. Thus our supposition is wrong. It is easy to observe that none of the members of $GF(2^n)$ used in the proof is zero or one, because λ is a root of an irreducible polynomial of degree at least 4. This completes the proof.

(D) Now we finally discuss the case when $p=7$ and $n\geqslant 2$, such that 3 does not divide n. In this case there are $\frac{p^n-p}{3}$ cubic residues belonging to $GF^*(p^n)-GF^*(p)$. show that these cubic residues cannot all belong to complete classes. If it were so, then by multiplying all members of G with 2 and 4 respectively it can be inferred that We all members of λG belong to complete classes and so do all members of $\lambda^2 G$. If this were true, then $\psi(\lambda)=\omega=\psi(\lambda+1)$, where λ is a generator of $GF^*(7^n)$. This means that $\psi(1+\frac{1}{\lambda})=1$ which means that $\psi(\frac{1}{\lambda})=1$. On the other hand $\psi\ (\frac{1}{\lambda})=\omega^2$ which follows from $\psi(\lambda)=\omega$. This contradiction enables us to conclude that all cubic residues in $GF^*(p^n)-GF^*(p)$ cannot belong to complete classes. Thus there exists α in $GF^*(p^n)-GF^*(p)$ such that $\psi(\alpha)=1$, and $\psi(\alpha+1)=\omega$.

Applying the previous method, we can decompose each member of λG as sum of two cubes. For expressing each member of $\lambda^2 G$ as sum of two cubes under this hypothesis, we first show that besides the condition of Lemma 2, anyone of the following conditions will also be sufficient for our purpose. The elements considered here belong to $GF^*(p^n)-GF^*(p)$.

(i) if there exists t such that $\psi(t)=\psi(t+1)=\omega$.

(ii) if there exists t_1 such that $\psi(t_1)=\psi(t_1+2)=\omega$ and $\psi(t_1+1)=1$.

In these two cases, $\psi(\frac{1}{t})=\omega^2$, $\psi(1+\frac{1}{t})=1$ and $\psi(t_1^2+2t_1)=\omega^2$, $\psi(t_1+1)^2=1$

Thus Lemma 2 is applicable. Considering our previous discussions, it is obvious that we can use any one of the four conditions for decomposition of each member of $\lambda^2 G$ as sum of two cubes. Besides Lemma 2 and these two conditions, the remaining condition relates to the existence of 3 members $\delta, \delta+1, \delta+2$ such that $\psi(\delta)=(\delta+2)=1$ and $\psi(\delta+1)=\omega$.

We proceed to consider all possible combinations for establishing the required part with the hypothesis that there exists α such that $\psi(\alpha)=1$ and $\psi(\alpha+1)=\omega$. If $\psi(\alpha+2)=1$ or ω, the above conditions stated will complete the proof. Thus we have to analyze the case further with $\psi(\alpha)=1$, $\psi(\alpha+1)=\omega$ and $\psi(\alpha+2)=\omega^2$. Since $(\alpha+6)$ and α are consecutive, therefore, if $\psi(\alpha+6)=\omega$ or ω^2, the above mentioned conditions again enable us to complete the proof. As a consequence, we consider $\psi(\alpha+6)=1$ and therefore $\psi(\alpha+5) \neq \omega^2$.

Since $\psi(\alpha+3)=1$ satisfies the condition of Lemma 2, therefore, we examine $\psi(\alpha+3)=\omega^2$ or ω. In what follows the explanation is given in regard to those cases where the above conditions are not satisfied.

Part 1 : There are two alternatives :

(i) $\psi(\alpha)=1, \psi(\alpha+1)=\omega, \psi(\alpha+2)=\omega^2, \psi(\alpha+3)=\omega^2, \psi(\alpha+4)=\omega,$
$\psi(\alpha+5)=1, \psi(\alpha+6)=1$

(ii) $\psi(\alpha)=1, \psi(\alpha+1)=\omega, \psi(\alpha+2)=\omega^2, \psi(\alpha+3)=\omega^2, \psi(\alpha+4)=\omega^2,$
$\psi(\alpha+5)=\omega, \psi(\alpha+6)=1.$

In (i), if $\psi(2)=\omega$, then $\psi(2\alpha+3)=\omega$, $\psi(2\alpha+4)=1$, $\psi(2\alpha+5)=\omega$ and we are done, if $\psi(2)=\omega^2$ then Lemma 2 can be used.

In (ii), if $\psi(2)=\omega$, we have $\psi(2\alpha+1)=1$, $\psi(2\alpha+2)=\omega^2$ and if $\psi(2)=\omega^2$, we make use of Lemma 2. This completes the argument.

Part 2: Here with $\psi(\alpha+3)=\omega$, we cannot have $\psi(\alpha+4)=\omega$ and so again we have two alternatives to consider:

(i) $\psi(\alpha)=1, \psi(\alpha+1)=\omega, \psi(\alpha+2)=\omega^2, \psi(\alpha+3)=\omega, \psi(\alpha+4)=1,$
$\psi(\alpha+5)=1, \psi(\alpha+6)=1.$

(ii) $\psi(\alpha)=1, \psi(\alpha+1)=\omega, \psi(\alpha+2)=\omega^2, \psi(\alpha+3)=\omega, \psi(\alpha+4)=\omega^2,$
$\psi(\alpha+5)=\omega, \psi(\alpha+6)=1.$

In (i) if $\psi(2)=\omega$, then $\psi(2\alpha)=\omega$ and $\psi(2\alpha+1)=\omega$ and if $\psi(2)=\omega^2$, Lemma 2 can be applied using integers 1 and 2.

In (ii) if $\psi(2)=\omega$, then $\psi(2\alpha+1)=1$, $\psi(2\alpha+2)=\omega^2$ and if $\psi(2)=\omega^2$, we make use of Lemma 2.

This takes care of all possible cases and the proof is complete

REFERENCES

Borevich, Z. I., and Shafarevich, I. R. (1966). Number Theory. Academic Press, New York.

Van der Waerden, B. L. (1970). Algebra, Volume 1. Frederick Ungar Publishing Company.