Al-Aqsa University Journal (Natural Sciences Series) , Vol.13, No.1, Pages 1-6, Jan. 2010
ISSN 2070-3155

لمحة عن نظرية العدد : دالة ضربية جديدة و نتيجة قديمة من نظرية الزمر

د. عبد الكريم ناجي*

أ. أحمد عبد الرحمن أبو ملوح **

الملخص

في هذه اللمحة نعرف دالة باستخدام مفهوم " الرتبة " للعدد x بمقياس العدد الطبيعي n ، ونبرهن أن هذه الدالة ضربية وسنبرهن بعض النتائج المتعلقة بهذه الدالة في نهاية هـذه الورقـة نبرهن نتيجة معروفة في الزمر الخاصة بالأعداد الصحيحة بمقياس معين :
وذلك بإثبات أن أعلى رتبة في (انظر: Gallian 2002, P.155) $U(2^k) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{2^{k-2}}$
الزمرة $U(2^k)$ هي 2^{k-2} .

A Note On Number Theory:"A New Multiplicative Function, And An Old Result In Group Theory

ABSTRACT

In this note we define a function using the concept of "order" of a number x modulo the natural number n, and show that this function is multiplicative. We also prove some results concerning this function.

At the end of this note we prove the well-know result in Group Theory : $U(2^k) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{k-2}}$ see [Gallian 2002 page 155] by showing that the highest order of an element in $U(2^k)$ is 2^{k-2} .

* قسم الرياضيات - كلية العلوم التطبيقية – جامعة الأقصى – غزة - فلسطين.

* قسم الرياضيات - الجامعة الإسلامية – غزة - فلسطين.

Definition 1. Let n be a positive integer. Define a function T : □ ® □ by $T(n)$ = number of elements x in $U(n)$ that satisfy x^2 ≡ 1 (mod n) , where $U(n) = \{ x : 1 \le x \le n$, gcd(x , n) = 1 }is the reduced residue system modulo n (or algebraically $U(n)$ is the group of units modulo n).

Lemma 1 Let $n > 2$. Then the product of elements of $U(n)$ is congruent to $(-1)^{\frac{T(n)}{2}}$ (modulo n).

proof: Write $U(n) = \{ r_1 , r_2 ,\ldots, r_{\frac{j(n)}{2}}, r_{\frac{j(n)}{2}+1},\ldots,r_{j(n)}\}$. For any i Î { 1 , 2 , … , $\frac{j(n)}{2}$ } we can find j in { $\frac{j(n)}{2}+1$, … , $j(n)$ } such that r_i ≡ - r_j (mod n) (This is ready from the fact that if k Î $U(n)$, then $n-k$ Î $U(n)$
If r_i satisfies r_i^2 ≡ 1 (mod n) then (r_j)^2 = (-r_i)^2 ≡ 1(mod n). Now let x be an element in U (n)) such that x^2 ≡ 1 (mod n) then $x \ne x^{-1}$ (where x^{-1} is the multiplicative inverse of x in $U(n)$) and the product of all such x is congruent to 1 (modulo n).
Therefore the product of all the elements of $U(n)$ is congruent to the product of the elements r_i that satisfy $x^2 \equiv 1$ (mod n) , and this is congruent to $(-1)^{\frac{T(n)}{2}}$ (mod n) .

In [3] (Guichard, 1999 P.139-142) showed that n has a primitive root when n is 1, 2 , 4 , p^k or $2p^k$ where p is an odd prime and $k \ge 1$ (r is a primitive root in $U(n)$ if r has order $\varphi(n)$)

Remark 1 : If n > 2 and n has a primitive root then U(n) contains exactly 2 elements x such that $x^2 \equiv 1$ (mod n) (*i.e* T(n) = 2) (this is because $U(n)$ is a cyclic group of order $\varphi(n)$ with 2 divides $\varphi(n)$, hence $U(n)$ contains only one subgroup of order 2).
In the next theorem we prove that $T(2^k) = 4$ for $k \ge 3$; which means that 2^k has no primitive root when $k \ge 3$. but first we state

Lemma 2 If p is a prime number and p^k divides ab where $k \ge 1$. then there exists i in

$\{0,1,\ldots k\}$ such that p^i divides a and p^{k-i} divides b.

Theorem 1 : If $k \geq 3$, then $T(2^k) = 4$

Proof : observe that the elements 1 , $2^{k-1} + 1$, $2^{k-1} - 1$, $2^k - 1$ all belong to $U(2^k)$ and satisfy $x^2 \equiv 1 \pmod{2^k}$ therefore $T(2^k) \geq 4$.

Now if $a \in U(2^k)$ and $a^2 \equiv 1 \pmod{2^k}$ then 2^k divides $a^2 - 1 = (a-1)(a+1)$.

Let i be the largest element in $\{0 , 1,\ldots,k\}$ such that 2^i divides $a - 1$ and 2^{k-i} divides $a + 1$ (by Lemma 2).

The cases $i = 0$, 1 , k , $k - 1$ will lead to elements 1 , $2^{k-1} + 1$, $2^{k-1} - 1$ and $2^k - 1$ which satisfy $x^2 \equiv 1 \pmod{2^k}$.

If $1 < i < k-1$, and $2^i \mid a - 1$ and $2^{k-i} \mid a + 1$ then there exists $s \in \mathbf{Z}$ such that $a = 2^i s + 1$

Thus $2^{k-i} \mid 2^i s + 2$ which means that

$2^{k-i-1} \mid 2^{i-1} s + 1$

and this is impossible since $k-i-1 \geq 1$.

Therefore , the case $1 < i < k - 1$ cannot happen , and this completes the proof.

In the next theorem we follow [Rosen 4 pages 209/210] to show that T is a multiplicative function.

Theorem 2 : T is a multiplicative function , that is ; if m and n are positive integers and gcd $(m, n) = 1$ then $T(mn) = T(m)T(n)$.

Proof: write the numbers from 1 to mn as follows :

1	2	3	…	r	…
m					
$m+1$	$m+2$	$m+3$	…	$m+r$	...
$2m$					
$2m+1$	$2m+2$	$2m+3$	…	$2m+r$	…
$3m$					
.	.	.		.	
.					
.	.	.		.	
.					

. . . .
.
$(n-1)m+1$ $(n-1)m+2$ $(n-1)m+3$ … $(n-1)m+r$ … nm

Each row is a complete residue system modulo m and each column is a complete residue system modulo n .
Thus each row (column) contains $T(m)$(resp. $T(n)$) of elements that satisfy $x^2 \equiv 1$ modulo m (resp. modulo n) with gcd $(x, mn)= 1$. This means that we have $T(m)$ of columns all of whose elements satisfy $x^2 \equiv 1 \pmod m$ (For if column r is such a one then each element of the column takes the form $km + r$. and $(km + r)^2 \equiv r^2 \equiv 1 \pmod m$) . Also , each such column contains $T(n)$ of elements satisfying $x^2 \equiv 1 \pmod n$.
So we have $T(m)\,.T(n)$ elements satisfying gcd (x, m) = gcd(x, n) = 1 and $x^2 \equiv 1 \pmod m$, $x^2 \equiv 1 \pmod n$, hence gcd(x, mn) = 1 and $x^2 \equiv 1 \pmod{mn}$. so we have $T(mn)= T(m)T(n)$.

Corollary : If $n = 2^k p_1^{a1} p_2^{a2} \ldots p_r^{ar}$ is written in the standard form (the prime factorization of n)then

$$T(n)=2^r.T(2^k)$$

$$= \begin{cases} 2^r, & k = 0 \text{ or } 1; \\ 2^{r+1}, & k = 2; \\ 2^{r+2}, & k \geq 3. \end{cases}$$

Proof : From Remark 1 we have $T(p_i^{ai}) = 2$. and from Theorem 1 . we have

$$T(2^k) = \begin{cases} 1, & k = 0 \text{ or } 1; \\ 2, & k = 2; \\ 4, & k \geq 3. \end{cases}$$

Theorem 3 : If n is a positive integer , then n has a primitive root if and only if the product of the elements of $U(n)$ is congruent to -1 (mod n),

Proof : Suppose n has a primitive root then $U(n)$ contains exactly one element of order 2 (see Remark 1) (i.e $T(n) = 2$), and by Lemma 1 ,

$\prod_{i \in U(n)} i = -1 \pmod{n}$.

Conversely suppose $\prod_{i \in U(n)} i = -1$ and assume that n has no primitive root . Then n is not of any of the forms 1 , 2 , 4 , p^k or $2p^k$ where p is an odd prime , $k \geq 1$. Therefore $n = u\upsilon$ where gcd $(u, \upsilon) = 1$, $u > 2$, $\upsilon > 2$ or $n = 2^k$, $k \geq 3$. In each case $T(n) = 2^s$, for some $s \geq 2$ (by the above corollary),and thus

$\prod_{i \in U(n)} i = (-1)^{\frac{T(n)}{2}} = (-1)^{2^{s-1}} \equiv 1 \pmod{n}$,

hence $n = 2$ which is not the case .

In [Burton, 2005, Exercise (8) page 162] it is shown that :

$a^{2^{k-1}} \equiv 1 \pmod{2^k}$

for all $a \in U(2^k)$, which means that the order of a is less than or equal to 2^{k-2} .Here we give a quit simple proof that $U(2^k) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{2^{K-2}}$, when $k \geq 3$.
We start the proof by showing that the element 5 has order 2^{k-2} in $U(2^k)$:

1. $5^{2^{k-2}} \equiv 1 \pmod{2^k}$.

By induction on $k \geq 3$: certainly the result is true when $k = 3$. Assume $5^{2^{k-2}} \equiv 1 \pmod{2^k}$. Then 2^k divides $5^{2^{k-2}} - 1$; say $5^{2^{k-2}} = 2^k r + 1$ for some r in $\mathbf{Z}$.
Then squaring $= 2^{2k} r^2 + 2^{k+1} r + 1 \equiv 1 \pmod{2^{k+1}}$ .Hence the result .

2. $5^{2^{k-3}} \neq 1 \pmod{2^k}$.

Claim: . $5^{2^{k-3}} \equiv 2^{k-1} + 1 \pmod{2^k}$

Proof of the claim: (by induction on k): For $k = 3$ it is clear .

Suppose $k \geq 3$ and $5^{2^{k-3}} \equiv 2^{k-1}+1 \pmod{2^k}$. Then $5^{2^{k-3}} - 2^{k-1} - 1 = 2^k M$ for some M.

We need to show that $5^{2^{k-2}} \equiv 2^k + 1 \pmod{2^{k+1}}$ or 2^{k+1} divides $5^{2^{k-2}} - 2^k - 1$. But $5^{2^{k-2}} - 2^k - 1 = (5^{2^{k-3}})^2 - 2^k - 1 = (2^k M + 2^{k-1} + 1)^2 - 2^k - 1 = 2^{2k} M^2 + 2^{2k} M + 2^{k+1} M +$
$2^{2k-2} \equiv 0 \pmod{2^{k+1}}$. Hence $5^{2^{k-2}} \equiv 2^k + 1 \neq 1 \pmod{2^{k+1}}$.

3. The order of 5 cannot be less than 2^{k+2}. For if order 5 is 2^r where $r < k-2$, then $r \leq k - 3$ and 2^r divides 2^{k-3} which means that $5^{2^{k-3}} = (5^{2^r})^m$, for some m and $5^{2k-3} \equiv 1^m \equiv 1 \pmod{2^k}$, a contradiction.

4. Finally, 2^{k-2} is the highest order in the group $U(2^k)$.
Therefore: $U(2^k) \cong \langle 5 \rangle \oplus \langle 5^{k-2} \rangle \cong \mathbf{Z}_{2^{k-2}} \oplus \mathbf{Z}_2$.

References

1. David M.Burton , Elementary Number Theory , 6th Ed . Mc Graw Hill 2005.
2. Joseph A. Gallian , contemporary Abstract Algebra , 5th Ed., Houghton MifflinCompany , 2002.
3. David R. Guichad , " When is $U(n)$ Cyclic ? An Algebra Approach ". Mathematics Magazine 72 (1999) : 139-142.
4. Kenneth H. Rosen , Elementary Number Theory Its Applications , 3rd Ed.. Ad-dision Weslay (57889) , 1993.