INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A09

# AN IDENTITY INVOLVING MULTIPLICATIVE ORDERS

**Marian Deaconescu**
*Department of MCS, Kuwait University, Kuwait*
deacon@mcs.sci.kuniv.edu.kw

*Received: 9/10/07, Revised: 1/31/08, Accepted: 2/5/08, Published: 2/18/08*

**Abstract**

An identity involving multiplicative orders is obtained by elementary combinatorial methods. Several classic and new results are obtained as direct consequences, including a characterization of the Mersenne primes.

*–Dedicated to Dan Daianu*

## 1. Introduction

Throughout this paper, $a, m, n$ are positive integers, $(a, m)$ denotes the greatest common divisor of $a, m$ and $\phi$ stands for Euler's totient function. If $X$ is a finite set, $|X|$ denotes the cardinality of $X$.

When $(a, m) = 1$, let $a_m$ denote, for strictly typographical purposes, the multiplicative order of $a$ modulo $m$. That is, $a_m$ is the smallest positive integer $k$ such that $m|a^k - 1$. Lagrange's theorem implies that $a_m$ divides $\phi(m)$ and therefore $i_a(m) := \sum_{d|m} \frac{\phi(d)}{a_d}$ is an integer.

When $p$ is a prime and $(a, p) = 1$, then $i_a(p) = 1 + \frac{p-1}{a_p}$. The well-known conjecture of E. Artin, asserting that whenever $a$ is not a square and $a \neq -1$ there exist infinitely many primes $p$ such that $a_p = p - 1$ can be elegantly stated in terms of $i_a(m)$: it states that there are infinitely many primes $p$ satisfying $i_a(p) = 2$.

The quantity $i_a(m)$ has an interesting number theoretical interpretation in a special case: when $p$ is a prime and $(m, p) = 1$, then $i_{p^k}(m)$ is the number of (distinct) irreducible factors of the polynomial $X^m - 1$ over the field $GF(p^k)$ – see Lemma 5 of [4].

The quantity $i_a(m)$ has gained in interest recently due to an interesting result of D. Ulmer – see Th. 9.2 of [8]: $i_a(m)$ is involved in the formulae for the ranks of certain elliptic equations over function fields. A forthcoming paper of C. Pomerance and I.E. Shparlinski [5], obtainable from C. Pomerance's site, studies $i_a(m)$ on average by using analytical methods. For more examples showing the rôle of $i_a(m)$ in other contexts, see also [6,9]. Since $i_a(m)$ involves a function as irregular as the multiplicative order, it is desirable to relate it to much more regular functions.

The aim of this note is to express $i_a(m)$ when $a > 1$ and $m \geq 1$ are *arbitrary* coprime integers in terms of the divisors of $a_m$. This is done by using a versatile combinatorial tool:

**Cauchy-Frobenius identity.** *Let $X$ be a finite nonempty set, let $G$ be a group of permutations acting on $X$ and for $g \in G$ denote by $C_X(g)$ the set of fixed points of $g$ in $X$. Then*

$$t|G| = \sum_{g \in G} |C_X(g)|,$$

*where $t$ is the number of orbits of the action of $G$ on $X$.*

When $X$ is a finite group and when $G$ is a group of automorphisms of $X$, then by Lagrange's theorem the integers $|C_X(g)|$ are divisors of $|X|$ for all $g \in G$. The simplest situation is that of $X$ and $G$ both being cyclic groups, for the algebraic structure of these groups is very well understood. However, the humble cyclic groups encapsulate a lot of interesting number – theoretical information and one may hope to uncover some of it by applying the Cauchy-Frobenius identity coupled with elementary group – theoretical considerations. This approach is not new, for a recent example see Isaacs and Pournaki [2]. We are going here a bit further, with the precise goal of obtaining explicit identities.

The main result of this paper is an identity expressing $i_a(m)$ in a somewhat more convenient way:

**Theorem.** *If $a > 1, m \geq 1$ and $(a, m) = 1$, then*

$$\sum_{d | a_m} \phi(\frac{a_m}{d})(m, a^d - 1) = a_m i_a(m). \tag{1}$$

It is apparent from (1) that $i_a(m)$ depends in fact essentially on the divisors of $a_m$, which is a number much smaller than $m$ when $m$ is composite.

The most natural proof is presented here, in the sense that it gives an interpretation to the quantity $i_a(m)$. It shows that $i_a(m)$ is the number of orbits in the action of a cyclic group of automorphisms acting on a cyclic group – this observation already appears (implicitly and independently) in the proof of Th. 9.2 of [8].

T. Ward has proofs of various divisibility results by using the theory of dynamical systems – his home page contains many downloadable papers related to the interplay between dynamical systems and number theory and J.H. Silverman's new book [7] is a good introduction to this field. Orbit counting for various actions is a very active field of research.

## 2. Proof of the Theorem

Let $Z_m = Z/mZ$ denote the ring of residue classes modulo $m$. By a slight abuse of notation, $Z_m = \{k|0 \leq k \leq m-1\}$ and it is understood that addition and multiplication are performed modulo $m$. The group of units of $Z_m$ is $U = \{u \in Z_m|(u,m) = 1\}$, $|U| = \phi(m)$ and since by hypothesis $(a,m) = 1$ we see that $a \in U$. Multiplication by $a$ induces an automorphism $\alpha$ of the additive group $Z_m$: $\alpha(k) = ak$ for all $k \in Z_m$. For simplicity of notation, write $a_m = n$, so that $|\alpha| = a_m = n$.

The group $G = \langle\alpha\rangle$ acts as a permutation group on $Z_m$ and $|G| = n$. For $d|n$, the order of $\alpha^d$ is $\frac{n}{d}$. Let $C_{Z_m}(\alpha^d) = \{k \in Z_m|a^d k = k\}$ denote the fixed point subgroup of $\alpha^d$ in $Z_m$. Then $C_{Z_m}(\alpha^d) = \{k \in Z_m|\ m|k(a^d-1)\} = \{k \in Z_m|\ \frac{m}{(m,a^d-1)}|k\} = \langle\frac{m}{(m,a^d-1)}\rangle$ and therefore $|C_{Z_m}(\alpha^d)| = (m, a^d-1)$.

There are exactly $\phi(\frac{n}{d})$ elements of $G$ of order $\frac{n}{d}$ and if $t$ denotes the number of orbits of the action of $G$ on $Z_m$ then, by the Cauchy-Frobenius identity, one obtains that

$$tn = \sum_{d|n} \phi(\frac{n}{d})(m, a^d-1). \tag{2}$$

What we have to do now is to express the value of $t$ in a different way. For every divisor $d$ of $m$, consider the set $X_d$ of all elements of order $d$ of the cyclic (additive) group $Z_m$. Then $|X_d| = \phi(d)$ and clearly $X_d$ is left invariant by the action of $G$. For $x \in X_d$, consider the orbit $O(x) = \{a^i x|1 \leq i \leq n\}$ of $x$ under the action of $G$. Then $|O(x)|$ is the least positive integer $s$ such that $x = a^s x$. For this $s$ we have (in $Z_m$) that $(a^s-1)x = 0$, whence $d = |x|$ divides $a^s - 1$. But by the definition of $s$ it follows that in fact $|O(x)| = a_d$ is just the multiplicative order of $a$ modulo $d$.

Thus, for every $x \in X_d$ we have $|O(x)| = a_d$ and therefore $G$ has exactly $\frac{\phi(d)}{a_d}$ orbits in $X_d$. Finally, sum up over the set of all divisors of $m$ to get

$$t = \sum_{d|m} \frac{\phi(d)}{a_d}. \tag{3}$$

Since the statement follows now from (2) and (3), the proof is complete.

## 3. Applications

The general identity (1) is the source of many interesting consequences. Let $a > 1$, $n \geq 1$. Then $(a, a^n-1) = 1$ and $a_{(a^n-1)} = n$, so taking $m := a^n - 1$ in (1) gives at once:

**Corollary 1.** *If $a > 1$ and $n \geq 1$, then*

$$\sum_{d|n} \phi(\frac{n}{d})(a^d-1) = ni_a(a^n-1) \ = \ n \sum_{d|a^n-1} \frac{\phi(d)}{a_d}. \tag{4}$$

*Remarks.* (1) By taking $n = 1$ in (4) one obtains Gauss' identity: if $a > 1$, then $a - 1 = \sum_{d|a-1} \phi(d)$; (2) Fermat's "little" theorem follows from (4) if one takes $n$ to be a prime.

**Corollary 2.** *If $a > 1, m \geq 1$ are coprime, then $(m, a-1)$ divides $a_m i_a(m)$.*

*Proof.* It suffices to observe that in the left hand side of (1) we have $(m, a-1) \mid (m, a^d - 1)$ for every divisor $d$ of $a_m$. $\square$

**Corollary 3.** *Let $a, m > 1$ and let $p$ be a prime such that $a^p \equiv 1 \pmod{m}$. Then $m \equiv (m, a-1) \pmod{p}$.*

*Proof.* It is clear that $a_m \in \{1, p\}$. When $a_m = 1$, one obtains by (1) that $m \equiv (m, a-1) = m \pmod{p}$. When $a_m = p$, one derives from (1) that $p \mid (p-1)(m, a-1) + m$, whence the result. $\square$

A well-known result of MacMahon [3] - see also [1], p. 192, - states that for $a, n > 0$ we have $n | \sum_{d|n} \phi(\frac{n}{d}) a^d$. The next result implies at once MacMahon's result and says a bit more:

**Corollary 4.** *If $a > 1, n \geq 1$ , then $\sum_{d|n} \phi(\frac{n}{d}) a^d = n(1 + i_a(a^n - 1))$.*

*Proof.* This follows at once from (4) and from Gauss' identity $n = \sum_{d|n} \phi(\frac{n}{d})$. $\square$

In fact, the identity in the above corollary makes it possible to obtain another type of divisibility result, one that shows that $a$ (and *not* $n$) divides a certain sum.

**Corollary 5.** *Let $a, n > 1$ be coprime. Then $a | \sum_{d|a^n-1, d\nmid a-1} \frac{\phi(d)}{a_d}$.*

*Proof.* Use first Corollary 4 to get $a \mid n(1 + i_a(a^n - 1))$, then use the fact that $(a, n) = 1$ to derive $a | 1 + i_a(a^n - 1)$. Now $1 + i_a(a^n - 1) = 1 + \sum_{d|a-1} \frac{\phi(d)}{a_d} + \sum_{d|a^n-1, d\nmid a-1} \frac{\phi(d)}{a_d} = 1 + (a-1) + \sum_{d|a^n-1, d\nmid a-1} \frac{\phi(d)}{a_d}$ and the result follows. $\square$

*Remark.* Corollary 5 does not always hold if $(a, n) > 1$: just take $a = 4, n = 2$.

A Mersenne prime is a prime of the form $a^n - 1$ where $a, n > 1$. Elementary considerations show that in fact one must have $a = 2$ and $n$ a prime. The following result is perhaps the first characterization of the Mersenne primes by a number theoretical property.

**Corollary 6.** *If $a, n > 1$, then*

$$\sum_{d|n} \phi(\frac{n}{d})(a^d - 1) \geq \sum_{d|n} \frac{n}{d} \phi(a^d - 1)$$

*and the equality holds if and only if $a^n - 1$ is a Mersenne prime.*

*Proof.* Let $D(k)$ denote the set of all positive divisors of $k$. Write $D(a^n-1) = A \cup B$, where $A = \{a^d - 1 \mid d|n\}$ and $B = D(a^n-1) \setminus A$. Observe that for $a^d - 1 \in A$ we have $\frac{\phi(a^d-1)}{a_{(a^d-1)}} = \frac{\phi(a^d-1)}{d}$.

Next, write the right hand side sum in (4) as $S_1 + S_2$, where $S_1$ is the sum taken over the divisors of $a^n - 1$ belonging to $A$ and $S_2$ corresponds to the divisors of $a^n - 1$ belonging to $B$. Thus, the right hand side of the identity (4) now reads $nS_1 + nS_2$ and by the above remarks $nS_1 = \sum_{d|n} \frac{n}{d}\phi(a^d-1)$. Hence $\sum_{d|n} \phi(\frac{n}{d})(a^d-1) - \sum_{d|n} \frac{n}{d}\phi(a^d-1) = nS_2 \geq 0$, proving the stated inequality.

Equality holds exactly when $S_2 = 0$, i.e., when $B = \emptyset$. By elementary arguments one can see that this happens precisely when $|D(a^n-1)| = |D(n)|$. This last equality occurs if and only if $a^n - 1$ is a (Mersenne) prime and the proof is complete. □

**Acknowledgments**

The author wishes to thank T. Albu, S. Rudeanu, J. Sándor and A. Zaharescu for remarks related to older versions of the manuscript. The warmest thanks to the referee, who detected several mistakes, stressed the importance of the quantity $i_a(m)$ and provided the references related to this topic.

**References**

1. B. Crstici and J. Sándor, *Handbook of Number Theory II*, Springer, 2006.
2. I.M. Isaacs and M.A. Pournaki, *Generalizations of Fermat's Little Theorem via group theory*, Amer. Math. Monthly **112** (2005), 734–740.
3. P.A. MacMahon, *Applications of the theory of permutations in circular procession to the theory of numbers*, Proc. London Math. Soc. **23** (1891–2), 305–313.
4. P. Moree and P. Solé, *Around Pelikán's conjecture on very odd sequences*, Manuscripta Math. **117** (2005), 219–238.
5. C. Pomerance and I.E. Shparlinski, *Rank statistics for a family of elliptic curves over a function field*, submitted for publication.
6. T.D. Rogers, *The graph of the square mapping on the prime fields*, Discrete Math. **148** (1996), 317–324.
7. J.H. Silverman, *The arithmetic of dynamical systems, Graduate Texts in Mathematics 241*, Springer, New York, 2007.
8. D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. **155** (2002), 295–315.
9. T. Vasiga and J. Shallit, *On the iteration of certain quadratic maps over GF(p)*, Discrete Math. **277** (2004), 219–240.