Generalizations of Carmichaels in a field extension

Kichul Kim
Dartmouth College

July 6, 2005

Abstract

The AKS conjecture states that $(\zeta - 1)^n \equiv \zeta^n - 1 \pmod{n}$ for ζ an r-th root of unity with r prime, only if n is a prime and $r \nmid n^2 - 1$. If n is a prime, n-th power map would be a Frobenius automorphism of $\mathbb{F}_n(\zeta)$, and thus the congruence will hold true. In general, n-th power map is not a field automorphism, but under suitable conditions, it can be a group automorphism of the multiplicative group of certain residue fields and their direct products. This leads to consider certain generalizations of the notion of Carmichael numbers to number rings.

1 Congruence in number rings

Definition 1.1. *A composite n is a Carmichael number if it satisfies*

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

for all integer a.

There are certain properties that a Carmichael number has, which I just state here.

- n is a Carmichael number <u>if and only if</u> it is square free and $(p-1)|(n-1)$ for each prime factor p of n.
- n is a Carmichael number <u>if and only if</u> $a^{n-1} \equiv 1 \pmod{n}$ for all integer a relatively prime to n.

We may generalize the notion of a Carmichael. Let L be a finite extension of $\mathbb{Q}$, and let $\mathcal{O}_L$ be the number ring in L. For an ideal I in the ring $\mathcal{O}_L$, $\|I\|$ indicates $|\mathcal{O}_L/I|$.

Definition 1.2. *A composite, squarefree ideal I is a Carmichael ideal if it satisfies*

$$\alpha^{\|I\|} \equiv \alpha \pmod{I}$$

for all $\alpha \in \mathcal{O}_L$.

Note that when $I = \mathfrak{p}$, a prime ideal in $\mathcal{O}_L$, the congruence naturally holds true for all $\alpha \in \mathcal{O}_L$. In this case, it is a simple statement that $\left(\mathcal{O}_L/\mathfrak{p}\right)^*$ is a cyclic group of order $\|\mathfrak{p}\| - 1 = p^f - 1$, where p is the prime under $\mathfrak{p}$ and f is the inertial degree of $\mathfrak{p}$ over p.

Interestingly, an ideal that satisfies the above definition enjoys properties analogous to those of a Carmichael number.

Proposition 1.1. *A composite, squarefree ideal $I \subset \mathcal{O}_L$ is a Carmichael ideal <u>if and only if</u> and $(\|\mathfrak{p}\| - 1)|(\|I\| - 1)$ for each prime ideal $\mathfrak{p}$ dividing I.*

Proof. ($\Rightarrow$) Suppose I is a Carmichael ideal. For some prime ideal $\mathfrak{p}$, there exists a generator β for the cyclic group $\left(\mathcal{O}_L/\mathfrak{p}\right)^*$. Thus,

$$\beta^{\|I\|} \equiv \beta \pmod{\mathfrak{p}}$$

Since $\beta \notin \mathfrak{p}$,

$$\beta^{\|I\|-1} \equiv 1 \pmod{\mathfrak{p}}$$

We get

$$(\|\mathfrak{p}\| - 1)|(\|I\| - 1)$$

($\Leftarrow$) Let $I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$. It suffices to show that

$$\alpha^{\|I\|} \equiv \alpha \pmod{\mathfrak{p}_i}$$

for all $\mathfrak{p}_i$, $1 \leq i \leq k$. For $\alpha \in \mathfrak{p}_i$, it is trivially true. Without loss of generality, assume $\alpha \notin \mathfrak{p}_i$. Then it remains to show that

$$\alpha^{\|I\|-1} \equiv 1 \pmod{\mathfrak{p}_i}$$

Since $\alpha^{\|\mathfrak{p}_i\|-1} \equiv 1 \pmod{\mathfrak{p}_i}$ and $(\|\mathfrak{p}_i\| - 1)|(\|I\| - 1)$, this completes the proof. $\square$

Proposition 1.2. *With notations defined as above, I is a Carmichael ideal <u>if and only if</u>*

$$\alpha^{\|I\|-1} \equiv 1 \pmod{I}$$

for all $\alpha \notin \mathfrak{p}_i$.

The proof of this proposition is very similar to the proof of the previous proposition.//

The arguments used in the proofs are analogous to those used to prove similar properties of a Carmichael number. Thus we may think that the properties of a Carmichael number are derived from its algebraic properties of the ring of rational integers, and those properties can be applied to a general number ring. From the above propositions, we can easily see that there are infinitely many Carmichael ideals, even though these belong to a particular category.

Proposition 1.3. *With the same notations above, if L is a normal extension, there are infinitely many Carmichael ideals.*

Proof. There are infinitely many primes in $\mathbb{Z}$ that are not primes L and also are unramified in L. That is, we can find infinitely many primes $p \in \mathbb{Z}$ such that $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ with $r > 1$ and prime ideals $\mathfrak{p}_i$. Thus we have $n = rf$. Notice that $\|p\mathcal{O}_L\| = (p^f)^r = p^n$, where f is the inertial degree of $\mathfrak{p}_i$ and n is the degree of the extension $L/\mathbb{Q}$. Then clearly $(\|\mathfrak{p}_i\| - 1)|(\|p\mathcal{O}_L\| - 1)$, since $\|\mathfrak{p}_i\| = p^f$ and $f|n$. $\square$

In a later section, I will show the same holds true for a general extension, not necessarily normal.

But this is an uninteresting example, since all such ideals would lie over a rational prime. Thus more interesting questions will be:

- Is there any composite ideal that lie above a rational composite?
- If there is, are there infinitely many such ideals in a given number ring?

I cannot answer these questions. But abusing the analogy with Carmicael numbers, I expect the answers to both questions to be affirmative.

But for now, I would like to demonstrate a possible connection of these ideals to the AKS conjecture. With the same notations as above, suppose there exists a rational integer n that satisfies the following:

- $n\mathcal{O}_L$ is a Carmichael ideal, where $L = \mathbb{Q}(\zeta_5)$.
- $ord_5(p) = 4$ for all prime $p|n$.

These two conditions would imply that $\alpha^{n^4} \equiv \alpha \pmod{n}$ for all $\alpha \in \mathbb{Z}[\zeta]$. In particular, $(\zeta - 1)^{n^4} \equiv \zeta - 1 = \zeta^{n^4} - 1 \pmod{n}$. But this is not quite what we want. However, we may gain some more information from the group structure of the multiplicative group of $\mathcal{O}_L/n\mathcal{O}_L$.

The two conditions imply that $\alpha^{n^4} \equiv \alpha \pmod{p}$ for all prime $p|n$. Since $\left(\mathcal{O}_L/p\mathcal{O}_L\right)^*$ is a cyclic group of order $p^4 - 1$, the congruence implies that if σ is a map that sends every element in $\left(\mathcal{O}_L/p\mathcal{O}_L\right)^*$ to its n-th power, σ is an automorphism of the group. That is,

$$\begin{aligned} \sigma : \left(\mathcal{O}_L/p_1\mathcal{O}_L\right)^* \cdots \left(\mathcal{O}_L/p_r\mathcal{O}_L\right)^* &\to \left(\mathcal{O}_L/p_1\mathcal{O}_L\right)^* \cdots \left(\mathcal{O}_L/p_r\mathcal{O}_L\right)^* \\ \alpha &\mapsto \alpha^n \end{aligned}$$

is a group automorphism. And σ has an order dividing f in $Aut(\left(\mathcal{O}_L/(n)\right)^*)$. So this may be seen as a weaker version of a Frobenius map that sends every element to its p-th power, when n is a prime p. In that case, the Frobenius map was a field automorphism that fixes $\mathbb{F}_p$. But here, what we have is just a group automorphism that does not necessarily fix $\mathbb{Z}/n\mathbb{Z}$.

But under a slightly stronger condition, Lenstra showed that n-th power map sends a particular element $\zeta - 1$ to what it would have been sent to under the Frobenius map when n is prime. Replacing the first condition above with $(p+1)|(n+1)$ for n a Carmichael number, the n-th power map acts on $\zeta - 1$ as if it were the Frobenius map.

2 Congruence in residue fields

Emboldened by the previous analogy, we may further venture to see if the same analogy would hold in the ring $\mathbb{F}_q[x]$. This ring, like the ring of rational integers, is a Euclidean domain and moding it out by a prime ideal gives us a finite field. Surprisingly, not only does the analogy hold, but it is closely related to Carmichael ideals.

Firstly, I show, in the following propositions, that there is a polynomial in the ring $\mathbb{F}_q[x]$ analogous to a Carmichael number in the ring of integers.

Proposition 2.1. *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial. Then*

$$g^{\|(f)\|} \equiv g \pmod{(f)}$$

for all $g \in \mathbb{F}_q[x]$, where (f) is the ideal in $\mathbb{F}_q[x]$ generated by f and $\|(f)\|$ is the size of the quotient ring $\mathbb{F}_q[x]/(f)$.

Proof. We may notice that $\|(f)\| = q^n$ where n is the degree of f. Since $\mathbb{F}_q[x]$ is UFD, f is a prime ideal in $\mathbb{F}_q[x]$. That is, $\mathbb{F}_q[x]/(f)$ is a field. Furthermore, it's finite, and its multiplicative group, $\left(\mathbb{F}_q[x]/(f)\right)^*$ is a cyclic group of order $q^n - 1$.

Now when $g \in (f)$, it is trivially true. Without loss of generality, assume $g \notin (f)$. It suffices to show that $g^{\|(f)\|-1} \equiv 1 \pmod{(f)}$, which is true because the multiplicative group has the order $q^n - 1$. This completes the proof. $\square$

This, in view of the previous effort, leads us to consider what can be called a "Carmichael polynomial" in $\mathbb{F}_q[x]$.

Definition 2.1. *Let f be a monic reducible polynomial. f is a Carmichael polynomial if*

$$g^{\|(f)\|} \equiv g \pmod{(f)}$$

for all $g \in \mathbb{F}_q[x]$, where $\|(f)\|$ is defined as above.

$\|(f)\|$ equals $q^{deg\, f}$. Thus if (g_1) and (g_2) are ideals in $\mathbb{F}_q[x]$, $\|(g_1 g_2)\| = \|(g_1)\| \cdot \|(g_2)\|$.

Proposition 2.2. *f is a Carmichael polynomial <u>if and only if</u>*

- *f is squarefree*
- *$(\|(g)\| - 1)|(\|(f)\| - 1)$ for all $g|f$.*

The proof is identical in structure to the proof of the properties of Carmichael numbers, except that now we are dealing with polynomials.

But notice that the second condition is equivalent to $d|n$ where d and n are degrees of g and f, respectively. That is,

- $\sum_{g|f} deg\, g = deg\, f$
- $(deg\, g)|(deg\, f)$

Thus in this case, we can easily see that there are infinitely many Carmichael polynomials, since if n is any multiple of a perfect number, we should be able to find a subset of its divisors whose sum equals itself. In particular, when the extension is normal, the two conditions above are equivalent and trivially true.

3 Correspondence

It is a known fact that the factorization of a prime p in a field extension L has a natural correspondence in $Z_p[x]$. I state without a proof the following theorem.

Theorem 3.1. *Let $L = \mathbb{Q}(\alpha)$ be an extension over Q for α an algebraic integer, and let g be the minimal polynomial for α over Q. Let $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i$ are prime ideals in $\mathcal{O}_L$ and $p \nmid |\mathcal{O}_L/\mathbb{Z}[\alpha]|$. Finally let $\overline{g}$ denote the image of g under the homomorphism*

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

with the map reducing each coefficient modulo p. Then,

$$\overline{g} = \overline{g_1}^{e_1} \cdots \overline{g_r}^{e_r}$$

and $f(\mathfrak{p}_i|p)$ is the degree of g_i. Moreover, $\mathfrak{p}_i = p\mathcal{O}_L + (g_i(\alpha))$.

This implies that if $p\mathcal{O}_L$ is a Carmichael ideal, then g is a Carmichael polynomial over $\mathbb{F}_p[x]$. This observation is not restricted to the case when the extension is normal, since the fact that $p\mathcal{O}_L$ is a Carmichael ideal implies that $p^{f_i} - 1 | p^n - 1$, where f_i is the inertial degree of $\mathfrak{p}_i$ over p, and n the degree of the extension. This is equivalent to $f_i | n$, and thus $\overline{g}$ is a Carmichael polynomial in $\mathbb{F}_p[x]$. Therefore, when $p\mathcal{O}_L$ is an unramified composite ideal in L, it is always a Carmichael ideal, slightly generalizing the previous proposition, but still not quite interesting. But we may be satisfied with the observation that given a Carmichael ideal, we can always find the corresponding Carmichael polynomial.

I hope that by using this correspondence I may be able to attack the conjecture in future efforts.