

Some observations on Problems #11, 12, and 13

Kichul Kim

Let n be an odd integer which is not a square and choose $D \in \mathbb{Z}$ so that $\left(\frac{D}{n}\right) = -1$. Define,

$$G = \{\alpha = a + b\sqrt{D} \in \mathbb{Z}/n\mathbb{Z}[\sqrt{D}] : N\alpha \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

$$H = \{\alpha \in G : \alpha^n \equiv \bar{\alpha} \pmod{n}\},$$

where $N\alpha$ is the norm of α , and $\bar{\alpha}$ is the conjugate of α in the ring $\mathbb{Z}/n\mathbb{Z}[\sqrt{D}]$. The definition of G may look different from what originally appeared in the problem list, but it is easy to observe that they are essentially the same.

The statement in question is: **For any D , a non-square modulo n , $G = H$ if and only if n is prime**

It is clear that when $n = p$ for some prime p , $\mathbb{Z}/p\mathbb{Z}[\sqrt{D}]$ forms a quadratic extension over $\mathbb{Z}/p\mathbb{Z}$ and thus p -th power map is, in fact, a non-trivial automorphism of $\mathbb{Z}/p\mathbb{Z}[\sqrt{D}]$, and thus $G = H$. So the interesting part of the question is under what conditions the converse might possibly hold true.

To restate the question, is it possible to find n such that $G = H$ for any non-square D ? I find that this is impossible for a composite n . But we can still ask a different question: for a composite n , does a number D exist such that $G = H$? Here I conclude, if such D exists, n has to be a Carmichael number such that $(p+1)|(n+1)$ for all primes $p|n$. And if such n exists, $G = H$.

Lemma 1. *If $G = H$ then n is prime or a Carmichael number.*

Proof. It may be seen as a diluted version of the original claim. Observe that $\forall s \in (\mathbb{Z}/n\mathbb{Z})^*$, $Ns = s^2 \in (\mathbb{Z}/n\mathbb{Z})^*$. Since $G \subseteq H$, $s^n \equiv \bar{s} = s \pmod{n}$, $\forall s \in (\mathbb{Z}/n\mathbb{Z})^*$. Therefore, n is either a Carmichael number or a prime. \square

From now, assume n is a Carmichael number. I will show that there exists D for which $G \neq H$.

Let $n = p_1 p_2 \dots p_k$. By the Chinese Remainder Theorem,

$$(\mathbb{Z}[x]/(x^2 - D, n))^* \cong (\mathbb{Z}[x]/(x^2 - D, p_1))^* \oplus (\mathbb{Z}[x]/(x^2 - D, p_2))^* \oplus \dots \oplus (\mathbb{Z}[x]/(x^2 - D, p_k))^*$$

Let $p = p_1$ and choose D such that $\left(\frac{D}{p}\right) = 1$. Then,

$$(\mathbb{Z}[x]/(x^2 - D, p))^* \cong \mathbb{Z}_p^* \oplus \mathbb{Z}_p^*$$

Indeed $\mathbb{Z}[x]/(x^2 - D, p) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ as rings. To see this, let $D \cong c^2 \pmod{p}$ and look at the map $\mathbb{Z}[x]/(x^2 - D, p) \rightarrow \mathbb{Z}_p \oplus \mathbb{Z}_p$ given by $a + bx \mapsto (a + bc, a - bc)$.

The norm of (u, v) in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is uv and the conjugate of (u, v) is (v, u) . Thus the p -component of H is the subgroup of $\mathbb{Z}_p^* \oplus \mathbb{Z}_p^*$ with $u^n = v$ and $v^n = u$. If we assume n is Carmichael, this simplifies to $u = v$, so H is not G .

Now if D is not a square modulo any of the primes dividing n , would there exist a number n such that $G = H$? In this case, $(\mathbb{Z}[x]/(x^2 - D, p)) \cong \mathbb{F}_{p^2}$, where \mathbb{F}_{p^2} is a finite field with characteristic p with p^2 elements. Consider the following homomorphism:

$$\sigma : \mathbb{F}_{p^2}^* \rightarrow \mathbb{Z}_p^*$$

$$\alpha \mapsto N\alpha$$

taking the norm of the elements. The map is onto, since for any $k \in \mathbb{Z}_p^*$, there exists $p + 1$ solutions to the equation $x^2 - Dy^2 = k$ in \mathbb{F}_p . This also leads to the fact that $|\ker \sigma| = p + 1$. Since we know that $\mathbb{F}_{p^2}^*$ is a cyclic group, and the kernel is a subgroup of it, we conclude that the kernel is also cyclic. So if the n th power map sends all elements in $\mathbb{F}_{p^2}^*$ to its conjugate we should have

$$\alpha^n = \bar{\alpha} = \alpha^{-1},$$

which is equivalent to $\alpha^{n+1} = 1$ for all $\alpha \in \ker \sigma$. Therefore $(p + 1)|(n + 1)$, for all $p|n$. If we can find such n , then n is a number for which $G = H$. Such a number has not been found yet.