D. Richman **On q-th power residues** Dec. 87

Let q denote a prime number. Recently Michael Rosen told me that if u and v are integers such that, for almost every prime p, either u or v is congruent modulo p to a q-th power, then either u or v is a q-th power. The Corollary to Proposition 2 below describes a generalization of this result.

Let Q denote the set of rational numbers.

Lemma 1 Let ζ denote a primitive q-th root of 1.

(i) If c is a rational number and c is a q-th power of an element of $Q[\zeta]$, then c is a q-th power of a rational number.

(ii) Let S denote a finite set of non-zero rational integers and let T denote the set of all q-th roots of elements of S. Suppose that there is an element of the Galois group of $Q[T]$ over $Q[\zeta]$ which does not fix any element of T. Then the set of rational primes p such that no element of S is congruent modulo p to a q-th power has density strictly bigger than 0.

Proof. If $q=2$, then $\zeta=-1$ and $Q[\zeta]=Q$, so statement (i) holds trivially. Suppose now that q is an odd prime, and suppose also that there is an element γ in $Q[\zeta]$ such that $\gamma^q=c$. Let N denote the norm map from $Q[\zeta]$ to Q and observe that $|N(\gamma)| = |\gamma|^{q-1}$ because the roots of X^q-c have the same absolute values. Since $|\gamma|^{q-1} = |N(\gamma)| \in Q$ and $|\gamma|^q = |c| \in Q$, $|\gamma| \in Q$. Therefore $|c|$ is the q-th power of a rational number, namely $|\gamma|$. This observation and the assumption that q is odd imply that c is the q-th power of a rational number. This proves (i).

Suppose that there is an element σ of the Galois group of $Q[T]$ over $Q[\zeta]$ such that $\sigma(t)-t \neq 0$ for every t in T. Let R denote the ring of algebraic integers in $Q[T]$. Let P denote an ideal of R such that P is a maximal ideal, P does not contain any element of $S\cup\{q\}$ and $\sigma(P)=P$. Since $t^q \in S$ for every element t in T, t^q is a rational integer and hence $\sigma(t)/t$ is a q-th root of 1 for every t in T. Observe also that $\sigma(t)/t \neq 1$ for every t in T. These observations and the assumption that P does not contain q imply that $\sigma(t)/t - 1$ does not lie in P when $t \in T$. Hence $\sigma(t)-t$ does not lie in P when $t \in T$; this observation and the assumption that $\sigma(P)=P$ imply that t is not congruent modulo P to a rational integer when $t \in T$. Therefore

(1) no element of S is congruent modulo P to a q-th power of a rational integer.

Note that only finitely many maximal ideals of R contain an element of $S \cup \{q\}$. Note also that, by the Chebotarev density theorem, the set of maximal ideals P of R satisfying $\sigma(P)=P$ has strictly positive density. These observations imply that the set of maximal ideals P of R for which statement (1) holds has strictly positive density. Therefore the set of rational primes p such that no element of S is congruent modulo p to a q-th power has strictly positive density. ▒

Proposition 2 Let S denote a set of rational integers. Assume that $|S| \leq q$ and S does not contain a q-th power of a rational integer. Then the set of primes p such that no element of S is congruent modulo p to a q-th power has density strictly bigger than 0.

Proof. Let T denote the set of q-th roots of elements of S, and let ζ denote a primitive q-th root of 1. Let G denote the Galois group of $Q[T]$ over $Q[\zeta]$, and for every element s in S, let $G(s) = \{\sigma \in G : \sigma$ fixes every q-th root of $s\}$. Since S does not contain a q-th power of a rational integer, statement (i) of the Lemma implies that S does not contain a q-th power of an element of $Q[\zeta]$. Therefore $G(s)$ is a proper subset of G for every s in S. Note also that if $s \in S$ and $t^q=s$, then $G(s)$ is the kernel of the homomorphism from G to $\{1, \zeta, \ldots, \zeta^{q-1}\}$ which maps σ to $\sigma(t)/t$. Therefore the index of $G(s)$ in G is q, so

$$(2) \qquad |G(s)| = |G|/q.$$

Observe that

$$\begin{aligned} \Big| \bigcup_{s\in S} G(s) \Big| &\leq 1 + \sum_{s \in S} \big| G(s) - \{1\} \big| \\ &= \text{(by (2))} \ 1 + |S|(|G|/q - 1) \\ &\leq \text{(since } |S| \leq q) \ 1 + |G| - q \end{aligned}$$

$< \quad |G|.$

Therefore there is an element of G which does not fix any element of T. Therefore statement (ii) of the Lemma implies that the set of primes p such that no element of S is congruent modulo p to a q-th power has density strictly bigger than 0. ▒

Corollary Let S denote a set of rational integers such that $|S| \leq q$ and, for almost every prime p, there is an element of S which is congruent modulo p to a q-th power. Then S contains a q-th power of a rational integer.

Remarks The Corollary does not hold when the size of S is strictly greater than q. For example let $S = \{ u, u^m v : 0 \leq m < q \}$, where u and v denote distinct primes. Then $|S| = q+1$ and, for every prime p, there is an element of S which is congruent modulo p to a q-th power, but S does not contain a q-th power.

More generally let k denote an integer such that $k \geq 2$ and let u and v denote distinct primes. Let $S = \{ u^d, v^d, u^m v : 0 < d < k, 0 < m < k,$ d divides k and $\gcd(m,k)=1 \}$. Then for every prime p, S contains a number which is congruent modulo p to a k-th power, but S does not contain a k-th power.