J. Number Theory 124(2007), no. 1, 57–61.

SIMPLE ARGUMENTS ON CONSECUTIVE POWER RESIDUES

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/~zwsun

Abstract. By some extremely simple arguments, we point out the following: (i) If n is the least positive kth power non-residue modulo a positive integer m, then the greatest number of consecutive kth power residues mod m is smaller than m/n. (ii) Let O_K be the ring of algebraic integers in a quadratic field $K = \mathbb{Q}(\sqrt{d})$ with $d \in \{-1, -2, -3, -7, -11\}$. Then, for any irreducible $\pi \in O_K$ and positive integer k not relatively prime to $\pi\bar{\pi} - 1$, there exists a kth power non-residue $\omega \in O_K$ modulo π such that $|\omega| < \sqrt{|\pi|} + 0.65$.

For an integer a relatively prime to a positive integer m, if the congruence $x^k \equiv a \pmod{m}$ is solvable then a is said to be a kth power residue mod m, otherwise a is called a kth power non-residue mod m. The theory of power residues (cf. [L]) plays a central role in number theory.

In this short note we aim to show that some classical topics on power residues can be handled just by some extremely simple observations.

Our first observation concerns the least positive kth power non-residue modulo a positive integer.

Theorem 1. (i) *Suppose that $n = n_k(m)$ is the least positive kth power non-residue modulo a positive integer m. Then the greatest number $R = R_k(m)$ of consecutive kth power residues mod m is smaller than m/n, consequently $n < \sqrt{m} + 1/2$ if m is a prime.*

(ii) *Let p be an odd prime, and let k be a positive integer with* $\gcd(k, p-1) > 1$. *Provided that -1 is a kth power residue mod p (i.e., $(p-1)/\gcd(k, p-1)$ is even) and that $n_k(p) \neq 2$, we have $n_k(p) < \sqrt{p/2} + 1/4$.*

Let p be an odd prime. That $n_2(p) < \sqrt{p} + 1$ was first pointed out by Gauss. Using sophisticated analytic tools, A. Granville, R. A. Mollin and H. C. Williams [GMW] proved that if $d > 3705$ is a discriminant of a quadratic number field then

---

2000 *Mathematics Subject Classification.* Primary 11A15; Secondary 05A19, 11A07, 11R11.

Partially supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and a Key Program of NSF (No. 10331020) in China.

the Kronecker symbol $(\frac{d}{q})$ is -1 for some prime $q < \sqrt{d}/2$; in particular, if $p > 3705$ is a prime with $p \equiv 1 \pmod 4$ then $n_2(p) < \sqrt{p/4}$.

Let k be a positive integer with $\gcd(k, p-1) > 1$. By a complicated elementary method, R. H. Hudson [Hud] proved that $n_k(p) < \sqrt{p/3} + 2$ if $p \neq 23, 71$. Let $N_k(p)$ denote the the greatest number of consecutive kth power non-residues mod p. By modifying our proof of Theorem 1 slightly, we can also show the following inequalities:

$$N_k(p) < \frac{p-1}{n_k(p)-1}, \quad R_k(p) \cdot \min\{R_k(p), N_k(p)\} < p, \quad R_2(p)N_2(p) < p.$$

A. Brauer [B] proved that $\max\{R_2(p), N_2(p)\} < \sqrt{p}$ for each prime $p \equiv 3 \pmod 4$. By a very sophisticated elementary approach, P. Hummel [Hum] confirmed in 2003 a conjecture of I. Schur by showing that $N_2(p) < \sqrt{p}$ except $p = 13$.

Proof of Theorem 1. (i) Suppose that all of $a+1, \ldots, a+R$ are kth power residues mod m where $a \in \mathbb{Z}$. Let q be the least integer greater than an/m. For any $i \in \{1, \ldots, R\}$, $(a+i)n - mq$ is a kth power non-residue mod m and hence

$$(a+i)n - mq \geqslant 0 \Longrightarrow (a+i)n - mq \geqslant n \Longrightarrow (a+i-1)n - mq \geqslant 0.$$

As $an - mq \ngeqslant 0$, we must have $(a+R)n - mq \ngeqslant 0$ and thus $nR < mq - an \leqslant m$. If m is a prime p, then $1, \ldots, n-1$ are kth power residues mod p, therefore $n(n-1) \leqslant nR \leqslant p-1 < p - 1/4$ and hence $n - 1/2 < \sqrt{p}$.

(ii) Write $p = 2nq + r$ with $q, r \in \mathbb{Z}$ and $0 < |r| < n = n_k(p)$. As $2nq = p - r$ is a kth power residue mod p, q must be a kth power non-residue mod p and hence $q \geqslant n$ since $q > 0$. Therefore $p \geqslant 2n^2 - (n-1)$ and thus $n - 1/4 < \sqrt{p/2}$. $\square$

Our second observation is the following new result established by our simple method used in the proof of Theorem 1(ii).

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \in \{-1, -2, -3, -7, -11\}$, and let O_K be the ring of algebraic integers in K. Let π be any irreducible element of O_K, and let k be a positive integer with $\gcd(k, N(\pi)-1) > 1$ where $N(\pi) = \pi\bar{\pi}$ is the norm of π with respect to the field extension $K/\mathbb{Q}$. Then there is a kth power non-residue $\omega \in O_K$ modulo π with $|\omega| < \sqrt{|\pi|} + 0.65$.*

Proof. It is well known that O_K is an Euclidean domain with respect to the norm $N: O_K \to \{0, 1, 2, \ldots\}$. (See, e.g., [ELS].) Thus O_K is a principle ideal domain and $O_K/(\pi)$ is a field with $N(\pi) = |\pi|^2$ elements. If $\alpha \in O_K$ is a kth power residue mod π, then $\alpha^{(N(\pi)-1)/d} \equiv 1 \pmod \pi$ where $d = \gcd(k, N(\pi)-1) > 1$. As the congruence $x^n \equiv 1 \pmod \pi$ over O_K has at most n solutions, there are kth power non-residues modulo π.

Let $\omega \in O_K$ be a kth power non-residue mod π with minimal norm. Then $N(\omega) < N(\pi)$ because $N(\omega - \eta\pi) < N(\pi)$ for a suitable $\eta \in O_K$.

Choose $\beta, \gamma \in O_K$ so that $\pi = \beta\omega + \gamma$ and $N(\gamma) < N(\omega) < N(\pi)$. If $\gamma = 0$, then ω is a unit since π is irreducible, hence $N(\omega) = 1 < |\pi| = \sqrt{N(\pi)}$ and so $|\omega| < \sqrt{|\pi|}$.

Now assume that $\gamma \neq 0$. Then $\pi \nmid \gamma$ since $N(\pi) \nmid N(\gamma)$. As $N(-\gamma) < N(\omega)$, $\beta\omega = \pi - \gamma$ is a kth power residue mod π and hence β must be a kth power non-residue mod π. So $N(\beta) \geqslant N(\omega)$, i.e., $|\beta| \geqslant |\omega|$. Note also that $|\gamma| < |\omega|$ since $N(\gamma) < N(\omega)$. Therefore $|\pi| \geqslant |\beta| \cdot |\omega| - |\gamma| > |\omega|^2 - |\omega|$. As

$$|\omega| = \sqrt{N(\omega)} \geqslant \sqrt{2} = \frac{c^2}{2c-1}$$

with $c = \sqrt{2} - \sqrt{2 - \sqrt{2}} = 0.6488...$, we have

$$|\pi| > |\omega|^2 - |\omega| \geqslant |\omega|^2 - 2c|\omega| + c^2 = (|\omega| - c)^2$$

and hence $|\omega| < \sqrt{|\pi|} + c < \sqrt{|\pi|} + 0.65$. This concludes the proof. $\square$

Concerning quadratic residues and non-residues, the law of quadratic reciprocity plays a central role. The general version of Gauss' lemma (cf. [S]), Euler's version of the law (cf. Proposition 5.3.5 of [IR]) and Scholz's proof of it (cf. [D, pp. 70-73]) via Gauss' lemma (this proof was rediscovered by the author in 2003), lead us to give our third theorem.

Theorem 3. *Let a, b, m, n be positive integers with $m - \varepsilon n = 2ab$ and* $\gcd(a, m) = \gcd(a, n) = 1$, *where ε is 1 or -1. Then we have the identity*

$$r_m(a) - \varepsilon r_n(a) = \left\lfloor \frac{a}{2} \right\rfloor b,$$

where

$$r_l(a) = \left| \left\{ 0 < r < \frac{l}{2} :\ r \in \mathbb{Z} \text{ and } \left\{ \frac{ar}{l} \right\} > \frac{1}{2} \right\} \right| \quad \text{for } \ l = 1, 2, 3, \dots ,$$

and $\lfloor \alpha \rfloor$ and $\{\alpha\}$ denote the integral part and the fractional part of a real number α respectively.

If the condition $\gcd(a, m) = \gcd(a, n) = 1$ in Theorem 3 is cancelled, then we can refine our proof of Theorem 3 to yield the following result:

$$\left| \left\{ 0 < r < \frac{m}{2} :\ r \in \mathbb{Z},\ \left\{ \frac{ar}{m} \right\} \geqslant \frac{1}{2} \right\} \right| - \varepsilon \left| \left\{ 0 < r < \frac{n}{2} :\ r \in \mathbb{Z},\ \left\{ \frac{ar}{n} \right\} \geqslant \frac{1}{2} \right\} \right|$$
$$= \begin{cases} \lfloor a/2 \rfloor b - \lfloor \gcd(a, n)/2 \rfloor & \text{if } \varepsilon = -1, \text{ and } n/\gcd(a, n) \text{ is odd;} \\ \lfloor a/2 \rfloor b & \text{otherwise.} \end{cases}$$

Proof of Theorem 3. As $\gcd(2a, m) \mid 2$, we have $2a \nmid sm$ for each positive integer $s < a$. Clearly

$$\begin{aligned} r_m(a) =& \sum_{s=0}^{a-1} \left| \left\{ \frac{s}{2a}m < r < \frac{s+1}{2a}m : \ r \in \mathbb{Z} \text{ and } \left\{ \frac{ar}{m} \right\} > \frac{1}{2} \right\} \right| \\ =& \sum_{s=0}^{a-1} \left| \left\{ r \in \mathbb{Z} : \ \frac{s}{2} < \frac{ar}{m} < \frac{s+1}{2} \text{ and } \left\{ \frac{ar}{m} \right\} > \frac{1}{2} \right\} \right| = \sum_{\substack{0 \leqslant s < a \\ 2 \nmid s}} \Delta_s(m), \end{aligned}$$

where

$$\begin{aligned} \Delta_s(m) =& \left| \left\{ r \in \mathbb{Z} : \ \frac{s}{2a}m < r < \frac{s+1}{2a}m \right\} \right| \\ =& \left| \left\{ r \in \mathbb{Z} : \ \varepsilon\frac{s}{2a}n < r - bs < \varepsilon\frac{s+1}{2a}n + b \right\} \right| \\ =& \left| \left\{ x \in \mathbb{Z} : \ \varepsilon\frac{s}{2a}n < x < \varepsilon\frac{s+1}{2a}n + b \right\} \right|. \end{aligned}$$

Similarly, $2a \nmid sn$ for every positive integer $s < a$, and

$$r_n(a) = \sum_{\substack{0 \leqslant s < a \\ 2 \nmid s}} \Delta_s(n)$$

with

$$\Delta_s(n) = \left| \left\{ r \in \mathbb{Z} : \ \frac{s}{2a}n < r < \frac{s+1}{2a}n \right\} \right| = \left| \left\{ x \in \mathbb{Z} : \ -\frac{s+1}{2a}n < x < -\frac{s}{2a}n \right\} \right|.$$

For any positive odd integer $s < a$, we have $2a \nmid (s+1)n$ (since $a \nmid s+1$ if $s < a-1$, and $2 \nmid n$ if $a = s+1 \equiv 0 \pmod 2$), hence

$$\Delta_s(m) - \varepsilon\Delta_s(n) = \left| \left\{ x \in \mathbb{Z} : \ \varepsilon\frac{s+1}{2a}n < x < \varepsilon\frac{s+1}{2a}n + b \right\} \right| = b.$$

Therefore

$$r_m(a) - \varepsilon r_n(a) = \sum_{\substack{0 < s < a \\ 2 \nmid s}} (\Delta_s(m) - \varepsilon\Delta_s(n)) = |\{0 < s < a : \ 2 \nmid s\}| \times b = \left\lfloor \frac{a}{2} \right\rfloor b.$$

This proves Theorem 3. $\square$

Acknowledgment. The author thanks the referee for his/her helpful comments.

References

[B] A. Brauer, *Über die Verteilung der Potenzreste*, Math. Z. **35** (1932), 39–50.

[D] H. Davenport, *The Higher Arithmetic*, 7th ed., Cambridge Univ. Press, Cambridge, 1999.

[ELS] R. B. Eggleton, C. B. Lacampagne and J. L. Selfridge, *Euclidean quadratic fields*, Amer. Math. Monthly **99** (1992), 829–837.

[GMW] A. Granville, R. A. Mollin and H. C. Williams, *An upper bound on the least inert prime in a real quadratic field*, Canad. J. Math. **52** (2000), 369–380.

[Hud] R. H. Hudson, *On the least k-th power non-residue*, Ark. Mat. **12** (1974), 217–220.

[Hum] P. Hummel, *On consecutive quadratic non-residues: a conjecture of Issai Schur*, J. Number Theory **103** (2003), 257–266.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in mathematics; 84), 2nd ed., Springer, New York, 1990.

[L] F. Lemmermeyer, *Reciprocity Laws: from Euler to Eisenstein*, Springer, Berlin, 2000.

[S] Z. W. Sun, *Products of binomial coefficients modulo p^2*, Acta Arith. **97** (2001), 87–98.