ACTA ARITHMETICA
166.4 (2014)

On q-orders in primitive modular groups

by

Jacek Pomykała (Warszawa)

Introduction. The aim of this paper is to investigate the large orders of integers $b \le B$ in the group $\mathbb{Z}_p^*$ in q-aspect, where p and q are prime numbers such that $q \mid p-1$. This problem is related to searching for the smallest value of b that is not the qth power in $\mathbb{Z}_p^*$. As already shown by the particular case $q=2$, the problem has no good solution from the computational point of view, since the best known lower bound obtained via the Burgess [Bu] estimate for the least quadratic nonresidue modulo p is of order $p^{\theta+\epsilon}$ where $\theta = 1/(4\sqrt{e})$ with any $\epsilon > 0$.

However Ankeny's [An] well known result says that the least quadratic nonresidue modulo p is $\ll \log^2 p$ under the assumption of the Riemann Hypothesis for the zeros of L-functions $L(s,\chi)$ attached to Dirichlet characters χ modulo p. Under the same conjecture the analogous result holds true for all prime divisors $q \mid p-1$, namely the least b which is not a qth power modulo p is $\ll \log^2 p$.

In this paper we consider the related problem without the assumption of the Riemann Hypothesis. Namely we deal with primes p for which the interval $[1,B]$ includes no element of "large" q-order, where $q \mid p-1$. In this connection we consider the set of Dirichlet characters χ modulo p of order d, where $q \mid d \mid p-1$. The least character nonresidue b with $\chi(b) \notin \{0,1\}$ is related to the "exceptional" zero of the corresponding L-function $L(s,\chi)$ close to the vertical line $\operatorname{Re} s = 1$. Applying for them the density estimates we will prove that if d is relatively large then the corresponding "exceptional" prime p does not exist.Therefore we conclude that there exists a relatively small $b \le B$ with large (maximal) q-order for some $q \mid d$. The small values $b \le B$ are significant in cryptography, where the efficient construction of a modular

2010 *Mathematics Subject Classification*: 11R45, 11M41, 11M06, 11Z05.
Key words and phrases: Dirichlet characters, L-functions, least chacter nonresidues, Riemann hypothesis, modular groups, orders, complex roots of unity, deterministic algorithms in cryptography.

DOI: 10.4064/aa166-4-5

subgroup generator of $\mathbb{Z}_p^*$ is required. This is indicated more precisely in Remark 10 below.

Notation. Throughout the paper, $Q \geq 2$ is a positive integer and p is a prime number lying in the arithmetic progresion $p \equiv 1 \pmod{Q}$.

For a positive number $B > 1$ we will denote by $\langle B\rangle_p$ the subgroup of $\mathbb{Z}_p^*$ generated by all numbers $b \leq B$ with $p \nmid b$.

Conventionally, we denote by $\nu_q(m)$ the highest exponent in which q divides m, while $\operatorname{ord}_p b$ stands for the order of b modulo p. By the *q-order* of b we mean the value $q^{\nu_q(\operatorname{ord}_p b)}$.

We use the standard notation $\omega(m)$ for the number of distinct prime divisors of m, and $P^+(m)$ for the largest prime divisor of m.

Throughout the paper, χ denotes a Dirichlet character modulo p, and $L(s,\chi)$ the L-function attached to χ. By the *order* of χ we mean the least positive integer k such that χ^k is a principal character.

The *least character nonresidue* n_χ is by definition the largest integer m_0 such that $\chi(m)$ assumes only values in $\{0,1\}$ for $m < m_0$.

Let $\alpha \in [1/2,1]$ and $\beta > 0$. We denote by $R(\alpha,\beta)$ the region in the complex plane $\mathbb{C}$ defined by the inequalities

$$1 \geq \operatorname{Re} s \geq 1-\alpha, \qquad |\operatorname{Im} s| \leq \beta.$$

Conventionally, $N(\sigma,T,\chi)$ denotes the number of nontrivial zeros of $L(s,\chi)$ lying in the rectangle $R(1-\sigma,T)$ ($\sigma \in [1/2,1]$).

Main result. Let d be a divisor of $p-1$ greater than or equal to 2 and $\zeta = \zeta_d \neq 1$ be a fixed complex dth root of unity.

Definition 1. A prime $p \equiv 1 \pmod{d}$ is called (d,ζ,B)-*exceptional* if

$$\zeta \notin \chi([1,B]) \tag{1}$$

for all Dirichlet characters χ modulo p of order d.

If condition (1) holds for any $\zeta_d \neq 1$, we call p $(d,1,B)$-*exceptional* or briefly (d,B)-*exceptional*. Thus p is (d,B)-exceptional if and only if

$$\chi([1,B]) \subseteq \{0,1\}$$

for all Dirichlet characters of orders dividing d.

From now on we will focus on the primes $p \equiv 1 \pmod{Q}$ that are (d,ζ^i,B)-exceptional with d being a divisor of Q, for $i=0,1$. Let $S_i = S_i(Q,d,\zeta^i,B,x)$ stand for the number of primes $p \leq x$ with $p \equiv 1 \pmod{Q}$ that are (d,ζ^i,B)-exceptional ($i=0,1$). We will prove

Theorem 2. *There exists a positive absolute constant A such that for $i = 0, 1$ we have*

$$S_i = S_i(Q, d, \zeta^i, B, x) \ll \frac{\exp\left\{\frac{11}{2}\frac{\log x}{\log B}\log(d^i A\log x) + 14\log\log x\right\}}{d^{1-i}}$$

provided the following conditions are satisfied:

$$(A\log x)^5 \le B \le x; \tag{2}$$

for $i = 0$,

$$\exp\left\{\frac{\log B}{\log(A\log x)}\right\} \le Q \le x; \tag{3}$$

and for $i = 1$,

$$\max\{e^5, \exp((\log B)^{1/2})\} \le Q \le x, \tag{4}$$

$$\frac{\exp\left\{\frac{\log B}{\log Q}\right\}}{A\log x} < d \le \min\left(Q, \frac{B^{1/5}}{A\log x}\right). \tag{5}$$

The proof of Theorem 2 is based on the following four lemmas.

Lemma 3 (see [Mo1]). *Let $1 \ge \sigma \ge 4/5$, $T > 0$, and $x \ge 1$. Then*

$$\sum_{\substack{p\le x\\ p\ prime}} \sideset{}{^*}\sum_{\chi \bmod p} N(\sigma, T, \chi) \ll (x^2(T+2))^{2(1-\sigma)/\sigma}(\log x(T+2)^{14})$$

where the inner sum is over all nonprincipal Dirichlet characters modulo p.

Lemma 4 (see [Mo2, Theorem 1, p. 164]). *Let χ be a nonprincipal Dirichlet character modulo p. There exists an absolute constant $A > 0$ such that if*

$$\chi([1, B]) \subseteq \{0, 1\}$$

then there exists a zero ρ of $L(s, \chi)$ such that $\rho \in R(\delta, \delta^2\log p)$, where δ with $1/\log p \le \delta \le 1/5$ satisfies the equality

$$(A\delta\log p)^{1/\delta} = B.$$

Lemma 5 (see [Mo2, Theorem 2, p. 167]). *Let $\zeta \ne 1$ be any dth root of unity ($d > 1$) and assume that $\zeta \notin \chi([1, B])$ for any Dirichlet character modulo p of order d. Then there exists an absolute constant $A > 0$ such that $L(\rho, \chi^k) = 0$ for some $0 < k < d$ and $\rho \in R(\delta, d\delta^2\log p)$ where δ satisfies the equality*

$$(dA\delta\log p)^{1/\delta} = B.$$

Lemma 6. *Let $d \mid p-1$ and ψ be any Dirichlet character modulo p of order $p-1$. Then*

$$\psi^{(p-1)/d}([1, B]) \subseteq \{0, 1\} \;\Leftrightarrow\; \#\langle B\rangle_p \,|\, (p-1)/d.$$

Proof. Obviously it is sufficient to prove the above equivalence for the values $\psi^{(p-1)/d}(b)$ with $b \le B$, $p \nmid b$. Since ψ has order $p-1$, the equality $\psi^{(p-1)/d}(b) = 1$ is equivalent to the condition $b^{(p-1)/d} \pmod{p} = 1$ for all $b \le B$ with $p \nmid b$. The latter means that $\operatorname{ord}_p b \mid (p-1)/d$ for all $b \le B$ with $p \nmid b$, hence $\#\langle B\rangle_p \mid (p-1)/d$, as required.

Proof of Theorem 2. Let

$$\delta = \delta_i = \delta_{i,A}(d^i, B, x) = \frac{\log(Ad^i \log x)}{\log B} \tag{6}$$

and consider the function $N(1-\delta, T, \chi)$ counting the zeros of the Dirichlet L-function $L(s,\chi)$ in the rectangle $R(\delta, T)$ with $T = T_i = d^i\delta_i^2 \log x$.

If p is (d, ζ^i, B)-exceptional then $\zeta \notin \chi([1,B])$ when $i = 1$, and $\chi([1,B]) \subseteq \{0,1\}$ when $i = 0$. In the first case we apply we use Lemma 5, while in the second we use Lemma 4 above with

$$B = B(i) = (Ad^i \log x)^{1/\delta_i}, \qquad i = 0, 1. \tag{7}$$

In case $i = 1$ we have $\chi(b) \ne \zeta$ for all $b \le B = B(1)$, hence also for $b \le (Ad\delta \log x)^{1/\delta}$ ($\delta = \delta_1 \le 1$). This implies that there exists a zero ρ of $L(s,\chi)$ with some $\chi \pmod{p}$ of order d, contained in the rectangle $R = R(\delta, \delta^2 d \log x)$, where $\delta = \delta_1$ is defined by (6).

Concluding, there exists at least one character χ of order d with the corresponding zero of $L(s,\chi)$ contributing nontrivially to $N(\delta, \delta^2 d \log x, \chi)$.

We still have to check that δ is chosen properly, i.e.

$$\frac{1}{\log p} \le \delta \le \frac{1}{5}.$$

The right-hand inequality follows from the right-hand inequality of (5), while the left-hand one follows from the observation that the assumption $p \equiv 1 \pmod{Q}$ implies that $p > Q$, hence

$$\frac{1}{\log p} \le \frac{1}{\log Q} \le \frac{\log(Ad \log x)}{\log B} = \delta$$

by the left-hand inequality of (5). Moreover the left-hand inequality of (4) is consistent with the conditions (2) and (5).

In case $i = 0$ we apply Lemma 4 to see that for p which is $(d,1,B)$-exceptional we have $\chi(b) = \{1\}$ for all $b \le B = B(0)$ with $p \nmid b$ and all characters $\chi^k = (\psi^{(p-1)/d})^k$ with $1 \le k \le d-1$. By Lemma 4 each of the L-functions $L(s,\chi^k)$ has a zero $\rho \in R(\delta_0, \delta_0^2 d^0 \log x) = R(\delta_0, \delta_0^2 \log x)$, thus contributing nontrivially to $N(1-\delta_0, \delta_0^2 \log x, \chi)$. Here the required inequality for δ_0 follows from (2) and the left-hand inequality of (3).

Let us now consider the following sums $\sum_i$ $(i = 0, 1)$ related to the (d, ζ^i, B)-exceptional numbers:

$$\sum\nolimits_i = \sum_{\substack{p\le x,\, p\equiv 1\, (\mathrm{mod}\, Q)\\ (d,\zeta^i,B)\text{-exceptional}}} \sum\nolimits^*_{\chi \bmod p} N(1-\delta_i, \delta_i^2 d^i \log x, \chi).$$

In view of the above discussion we have

$$\sum\nolimits_1 \ge \sum_{\substack{p\le x,\, p\equiv 1\, (\mathrm{mod}\, Q)\\ (d,\zeta,B)\text{-exceptional}}} N(1-\delta_1, \delta_1^2 d \log x, \chi) \ge S_1(Q, d, \zeta, B, x)$$

and similarly

$$\sum\nolimits_0 \ge \sum_{\substack{p\le x,\, p\equiv 1\, (\mathrm{mod}\, Q)\\ (d,1,B)\text{-exceptional}}} (d-1) N(1-\delta_0, \delta_0^2 \log x, \chi) \ge (d-1) S_0(Q, d, 1, B, x).$$

Now we apply Lemma 3 to get an upper bound for $\sum_i$ $(i = 0, 1)$. We have

$$\begin{aligned}\sum\nolimits_i &= \sum_{p\le x} \sum\nolimits^*_{\chi \bmod p} N(1-\delta_i, T_i, \chi) = \sum_{p\le x} \sum\nolimits^*_{\chi \bmod p} N(1-\delta_i, \delta_i^2 d^i \log x, \chi)\\ &\ll (x^2(T_i+2))^{2\delta_i/(1-\delta_i)} (\log x (T_i+2))^{14}\\ &\ll (x^2 x^{1/5})^{5\delta_i/2} (\log x^{6/5})^{14} \ll x^{11\delta_i/2} (\log x)^{14}\\ &\ll \exp\biggl(\frac{11}{2}\,\frac{\log x}{\log B} \log(A d^i \log x) + 14 \log\log x\biggr).\end{aligned}$$

Applying the lower bounds for $\sum_0$ and $\sum_1$ we obtain the required bounds for $S_i(Q, d, \zeta^i, B, x)$, $i = 0, 1$.

Lemma 7 (see [PK]). *Let $x \ge 4$ and $2 \le y \le x$. Then*

$$\#\{m \le x : P^+(m) \le y\} > x^{1-\frac{\log\log x}{\log y}}.$$

A prime $p \equiv 1 \pmod d$ is called (d, B)-*admissible* if it is not (d, B)-exceptional. By Lemma 6 the prime p is (d, B)-admissible provided

$$\nu_q(\#\langle B\rangle_p) > \nu_q(p-1) - \nu_q(d) \tag{8}$$

for some prime number $q \mid d$. Let us define

$$\mathfrak{z}_A(x, B) := \exp\biggl(\frac{11}{2}\,\frac{\log x}{\log B} \log(A \log x) + 14 \log\log x\biggr). \tag{9}$$

Applying Theorem 2 for $i = 0$ we obtain

Corollary 8. *There exist absolute positive constants A, c such that if*

$$(A\log x)^5 \le B \le x, \tag{10}$$

$$\max\left\{\mathfrak{z}_A(x,B), \exp\left(\frac{\log B}{\log(A\log x)}\right)\right\} \le Q \le x, \tag{11}$$

$$d > c\mathfrak{z}_A(x,B), \qquad d \mid Q, \tag{12}$$

then every prime $p \le x$ with $p \equiv 1 \pmod{Q}$ is (d,B)-admissible.

Proof. Note that the conditions (10)–(11) imply the inequalities (2)–(3) of Theorem 2 and therefore by (12) we conclude that $S_0(Q,d,1,B,x) = 0$, as required.

In particular letting $d = Q$ we deduce that for B and d satisfying

$$(A\log x)^5 \le B \le \exp\big(\tfrac{11}{2}(\log x)^{1/2}\log(A\log x)\big), \tag{13}$$

$$d > c\mathfrak{z}_A(x,B), \tag{14}$$

any prime $p \le x$ such that $p \equiv 1 \pmod{d}$ is (d,B)-admissible.

The inequality (8) is tight if d itself is a prime power. On the other hand, if $Q/\mathfrak{z}_A(x,B)$ is relatively large one observes that the number of distinct q dividing d that satisfy (8) is at least as large as the number of pairwise coprime integers $d' \ge c\mathfrak{z}_A(x,B)$ dividing d. However, if $Q/\mathfrak{z}_A(x,B)$ is relatively small and $\omega(d)$ is relatively large, then the number of suitable prime q satisfying (8) can be estimated nontrivially with the aid of Lemma 7. Namely, let us denote by m_l the divisor of m composed of all lth powers of primes. We have the following

Proposition 9. *Let $l \ge 1$ be an integer. There exist absolute positive constants A, c, c' such that if B and d_l satisfy*

$$(A\log x)^5 \le B \le \exp\big(\tfrac{11}{2}(\log x)^{1/2}\log(A\log x)\big), \tag{15}$$

$$d_l > c\mathfrak{z}_A(x,B), \tag{16}$$

then for every prime $p \le x$ with $p \equiv 1 \pmod{d_l}$, the number of primes q dividing d_l such that

$$\nu_q(\#\langle B\rangle_p) > \nu_q(p-1) - l$$

is at least

$$\max\left(1, \omega(d_l) - c'\frac{\log x}{l\log B}\right)$$

provided $x \ge x_0(A,l)$ is sufficiently large.

Proof. By the upper bound for $S_0(Q,d_l,1,B,x)$ in Theorem 2 with $d = d_l = Q$, there exists an absolute constant $c > 0$ such that if

$$d_l > c\mathfrak{z}_A(x,B)$$

then the set of (d_l, B)-exceptional primes $p \leq x$ with $p \equiv 1 \pmod{d_l}$ is empty. Hence such a prime p is (d_l, B)-admissible, i.e. there exists a prime $q \mid d_l$ such that

$$\nu_q(\#\langle B\rangle_p) > \nu_q(p-1) - l,$$

which justifies the first term of the maximum above.

To improve the estimate for large values of $\omega(d_l)$ let us write

$$d_l = \prod_{i\leq s} q_i^{\nu_i} \prod_{i=s+1}^{r} q_i^{\nu_i} = d'd''$$

say, where $\nu_q(\#\langle B\rangle_p) \leq \nu_q(p-1)-l$ for $q \mid d'$, while $\nu_q(\#\langle B\rangle_p) > \nu_q(p-1)-l$ for $q \mid d''$. Then

$$(q_1 \ldots q_s)^l \mid \frac{p-1}{\#\langle B\rangle_p}.$$

Furthermore, $q_1 \ldots q_s$ is no smaller than the product of the first s consecutive primes, which is $\gg s^s$ in view of the prime number theorem. Now applying the lower bound of Lemma 7 and equality (9) we see that for sufficiently large $x \geq x_0(A, l)$,

$$\#\langle B\rangle_p \geq \#\{m < p : P^+(m) \leq B\} > p^{1-\frac{\log\log p}{\log B}} > (p-1)/p^{\frac{\log\log p}{\log B}}.$$

Therefore

$$s^{ls} \ll (q_1 \ldots q_s)^l \leq \frac{p-1}{\#\langle B\rangle_p} \leq p^{\frac{\log\log p}{\log B}} \leq x^{\frac{\log\log x}{\log B}},$$

and taking the logarithms of both sides we obtain

$$ls \log s \ll \frac{\log x}{\log B} \log\log x,$$

hence

$$s \ll \frac{1}{l} \frac{\log x}{\log B}$$

for sufficiently large $x \geq x_0(A, l)$.

Thus the number of q's dividing d such that $\nu_q(\#\langle B\rangle_p) > \nu_q(p-1) - l$ is at least

$$r - s \geq \max\left(1, \omega(d_l) - c'\frac{\log x}{l \log B}\right)$$

for some $c' > 0$, provided $x \geq x_0(A, l)$ is sufficiently large. This completes the proof of Proposition 9.

Remark 10. Let m be the smallest integer with $q^m > d > c\mathfrak{z}_A(x, B)$, where $1 \leq m \leq l$. We have two interesting special cases: $m = 1$ and $m = l = \nu_q(p-1)$. If $m = 1$ then there exists $b \leq B$ such that the q-order of b modulo p is maximal, i.e. $q^{\nu_q(p-1)} \mid \mathrm{ord}_p b$. If $m = l = \nu_q(p-1)$ then $q \mid \mathrm{ord}_p b$. Given q and B an interesting computational problem is to deterministically find p and $b \leq B$ such that $p \equiv 1 \pmod{q}$ and $q \mid \mathrm{ord}_q b$. This is a common challenge in the efficient generation of cryptographic system parameters (cf. e.g. ElGamal's cryptosystem [ElG]).

Acknowledgements. The author is grateful to the anonymous referee for the valuable remarks that helped to improve the presentation of the paper.

References

[An] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55 (1952), 65–72.

[Bu] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), 106–112.

[ElG] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, in: Advances in Cryptology (Santa Barbara, CA, 1984), Lecture Notes in Comput. Sci. 196, Springer, 1985, 10–18.

[Mo1] H. L. Montgomery, *Zeros of L-functions*, Invent. Math. 8 (1969), 346–354.

[Mo2] H. L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, CBMS Reg. Conf. Ser. Math. 84, Amer. Math. Soc., 1994.

[PK] C. Pomerance and S. Konyagin, *On primes recognizable in deterministic polynomial time*, in: The Mathematics of Paul Erdős, R. L. Graham and J. Nešetřil (eds.), Springer, 1997, 176–198.

Jacek Pomykała
Institute of Mathematics
Faculty of Mathematics, Informatics and Mechanics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: pomykala@mimuw.edu.pl

Received on 1.7.2014
and in revised form on 28.10.2014 (7859)