Least Quadratic Non-Residue assuming Weak GRH

Weaker Bound

This is a simple analysis to find the Least quadratic non residue in $\mathbb{F}_p$. The calculation is much less rigorous and the bound is a bit weaker $\{\ O(\log^4(p))\}$ as compared to that of Ankeny [1].

Notations

The least quadratic non-residue modulo prime p is denoted by $n(p)$. χ_o, χ_2 denotes the trivial and quadratic(1 on residues and -1 at non-residues) Dirichlet character respectively. $\psi(x) = \sum_{i \leq x} \Lambda(i)$ and $\Lambda(n) = \log p$ If $n = p^r$ for some prime p and 0 otherwise.

I will now state few basic facts of Analytic number theory. One can find proof of all these facts in [2].

Fact 1.
$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} + \frac{1}{2}\log(1 - x^{-2})$$
here ρ are the non-trivial roots of the Riemann zeta function.

Using Fact 1 it is easy to see that assuming *Riemann Hypothesis*

$$\psi(x) = x + O(\sqrt{x}\log^2 x)$$

Fact 2. *Let $\psi(x, \chi) = \sum_{i \leq x} \Lambda(i)\chi(i)$ and χ be a non-trivial character* mod p
$$\psi(x, \chi) = -\sum_{\rho} \frac{x^\rho}{\rho} - \frac{L'(0, \chi)}{L(0, \chi)} + \textit{ polylog(p)}$$
here ρ are the non-trivial roots of the Dirichlet L function.

Theorem 1. *Assuming GRH, $n(p) = O(\log^4 p)$.*

Proof. Consider

$$S(M) = \sum_{1 \le a \le M} \chi_o(a)\Lambda(a) - \sum_{1 \le a \le M} \chi_2(a)\Lambda(a)$$

Note that: $S(M)$ is positive iff there is a quadratic non residue in $[1, M]$.
We know,

$$\begin{aligned} S(M) &= \psi(M, \chi_o) - \psi(M, \chi_2) \\ &= M + O(M^{0.5} \log^2(pM)) \qquad \textit{(by GRH)} \end{aligned}$$

Since $S(M) > 0$, $M > CM^{0.5}log^2(Mp)$. Therefore $M = O(\log^4 p)$

□

Weaker Generalized Riemann Hypothesis

The Generalized Riemann hypothesis says all the non-trivial roots ρ of the Dirichlet L function are on real part $z = 0.5$, but what if we instead of assuming "the exact Riemann hypothesis" consider a weaker form of it. Instead of saying that all the non trivial roots lie on $RE(\rho) = 0.5$. We consider that all the non trivial roots lie in a smaller critical strip $[0.5 - \epsilon, 0.5 + \epsilon]$. So depending on ϵ will our bound will remain poly(log n) or becomes polynomial in n, that is the basic question to be encountered.
Using Fact 2 it is easy to see that

$$\psi(x, \chi) = O(x^{0.5+\epsilon} \log^2(pm))$$

Theorem 2. *In Case of weaker Generalized Riemann hypothesis,*

$$n(p) = O(\log^{\frac{4}{1-2\epsilon}} p)$$

Proof. Consider

$$S(M) = \sum_{1 \le a \le M} \chi_o(a)\Lambda(a) - \sum_{1 \le a \le M} \chi_2(a)\Lambda(a)$$

Again S(M) is positive iff there are no quadratic non residue in [1,M] We know,

$$\begin{aligned} S(M) &= \psi(M, \chi_o) - \psi(M, \chi_2) \\ &= M + O(M^{0.5+\epsilon} \log^2(pm)) \qquad \textit{(by weak GRH)} \end{aligned}$$

Since $S(M) > 0$, $M > CM^{0.5+\epsilon}log^2(Mp)$. Therefore $M = O(\log^{\frac{4}{1-2\epsilon}} p)$ □

]

Bibliography

[1] Ankeny, N. C. "The Least Quadratic Non Residue." Annals of Mathematics Second Series 55.1 (1952): 65-72. Web.

[2] Ram Murty, "Problems in Analytic Number Theory, Springer " , https://books.google.co.in/, publisher