A research on the minimum prime quadratic residue module a prime

Zhang Xiao　Ye Lizao　Fang Weijun
（Wenzhou Middle School　Class 1,Grade 3　Wenzhou, Zhejiang　325600）

Abstract: This paper estimates the upper bound of the minimum prime quadratic residue module a prime and gives the asymptotic formula of $\sum\limits_{\substack{p\le x\\ f(p)=r}} 1$ (r is a prime).

Key words: Prime; Quadratic residue; Upper bound; asymptotic formula.

Introduction: while learning number theory, we discovered the irregulation of the distribution of the prime quadratic residue module a prime. Hence we were looking forward to the upper bound of the minimum prime quadratic residue module a prime. It was the original intention of our research. After several months' research, we got a fairy good upper bound and some related conclusion.

If there is no special explanation, this paper adopts the terminologies and symbols in【1】.
We use the following definitions:

Definition 1 For odd prime p, the smallest prime r such that $\left(\frac{r}{p}\right)=1$ is called the minimum prime quadratic residue modulo p, written as $f(p)$.Here $\left(\frac{r}{p}\right)$ is Legendre Symbol, sic passim.

Definition 2 For prime r, positive integer k and integer a, for all $x>1$, define $\pi(x)=\sum\limits_{p\le x}1$; $\pi(x;k,l)=\sum\limits_{\substack{p\le x\\ p\equiv l(\mathrm{mod}\,k)}}1$; $\pi_r(x)=\sum\limits_{\substack{p\le x\\ f(p)=r}}1$.

Definition 3 For every positive integer m, we set $g_m(x)=x^2-x+m$.

This paper is going to demonstrate the following theorems:

Theorem 1 For every prime r, $\pi_r(x)\sim\frac{\pi(x)}{2^{\pi(r)}}(x\to\infty)$.

Theorem 2 For $n>41$, there is a integer k, $1\le k<\frac{1}{2}+\sqrt{\frac{n}{3}}$, and $g_n(k)$ is a composite number.

Theorem 3 For prime $p>163$, $f(p)<\sqrt{p}$.

Furthermore，we conjecture that for any $\varepsilon > 0, f(p) = O(p^{\varepsilon})$.

We need the following lemmas：

Lemma 1[1] (Law of Quadratic Reciprocity) For different odd primes p and q, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$.

Lemma 2[1] (Chinese Remainder Theorem) Suppose m_1, m_2 ,... m_k are positive integers which are pairwise coprime.，then for integers a_1, a_2 ,..., a_k ， the system of congruences $x \equiv a_j \left(\bmod m_j\right)$, $j = 1, 2, \cdots, k$, has exactly one solution modulo $m_1 m_2 \cdots m_k$.

Lemma 3[3] if $k > 0$， $(l, k) = 1$，then for all $x > 1$, $\pi(x; k, l) \sim \frac{\pi(x)}{\varphi(k)} (x \to \infty)$.

Lemma 4[1] (Fermat-Euler) For every prime p with the form $4k+1$, p is expressible as $p = x^2 + y^2$ with *x* and *y* positive integers.

Lemma 5[2] (G.Rabinovitch) For $m \ge 2$ and $x = 1, 2, \cdots, m-1$, $g_m(x)$ are always primes if and only if the class number of the imaginary quadratic field $K = Q\left(\sqrt{1-4m}\right)$ is 1.

Lemma 6[2] (Baker)there are only 9 imaginary quadratic fields $K = Q\left(\sqrt{-d}\right)$ whose class number is 1：d＝1，2，3，7，11，19，43，67，163.

The proof of Theorem 1:

It’s well known that $\left(\frac{2}{p}\right) = 1$ if and only if prime $p \equiv \pm 1 (\bmod 8)$.

And by Lemma1，for prime $p \equiv 5 (\bmod 8)$ and odd prime q, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$;

for prime $p \equiv 3 (\bmod 8)$ and odd prime q， $\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right)$.

For $r = 2$， by Lemma3，

$$\pi_2(x)=\sum_{\substack{p\le x\\ f(p)=2}}1=\sum_{\substack{p\le x\\ p\equiv\pm1(\bmod 8)}}1=\pi(x;8,1)+\pi(x;8,-1)\sim\frac{2\pi(x)}{\varphi(8)}=\frac{\pi(x)}{2^{\varphi(2)}}(x\to\infty)$$

For $r\ge 3$, suppose $p_1,p_2,\dots,p_n$ are the primes smaller than r and with the form $4k+1$, $q_1,q_2,\dots,q_m$ are the primes smaller than r and with the form $4k+3$.

Define the sets of quadratic nonresidue modulo p_i as $\left\{a_{i,d}:d=1,2,\cdots\frac{p_i-1}{2}\right\}, i=1,2,\cdots,n$.

Define the sets of quadratic nonresidue modulo q_j as $\left\{b_{j,d}:d=1,2,\cdots\frac{q_j-1}{2}\right\}, j=1,2,\cdots,m$.

Define the set of quadratic residue modulo r as $\left\{e_d:d=1,2,\cdots\frac{r-1}{2}\right\}$

Hence $f(p)=r\Leftrightarrow\left(\frac{2}{p}\right)=\left(\frac{p_i}{p}\right)=\left(\frac{q_j}{p}\right)=-1$ and $\left(\frac{r}{p}\right)=1$

$$\Leftrightarrow\begin{cases}p\equiv5(\bmod 8)\\ \left(\frac{p}{p_i}\right)=-1\\ \left(\frac{p}{q_j}\right)=-1\\ \left(\frac{p}{r}\right)=1\end{cases}\text{or}\begin{cases}p\equiv3(\bmod 8)\\ \left(\frac{p}{p_i}\right)=-1\\ \left(\frac{-p}{q_j}\right)=-1\\ \left(\frac{-p}{r}\right)=1\end{cases}\Leftrightarrow\begin{cases}p\equiv4+\alpha(\bmod 8)\\ p\equiv a_{i,u_i}(\bmod p_i), i=1,2,\cdots,n,\\ p\equiv\alpha b_{j,v_j}(\bmod q_j), j=1,2,\cdots,m,\\ p\equiv\alpha e_t(\bmod r)\end{cases}$$

for some $\alpha\in\{\pm1\}; u_i\in\left\{1,2,\cdots\frac{p_i-1}{2}\right\}, i=1,2,\cdots,n;$

$v_j\in\left\{1,2,\cdots\frac{q_j-1}{2}\right\}, j=1,2,\cdots,m; t\in\left\{1,2,\cdots\frac{r-1}{2}\right\}$ hold.

We set $M=8p_1p_2\cdots p_nq_1q_2\cdots q_mr$.

By Lemma2, the system of congruences $\begin{cases}x\equiv4+\alpha(\bmod 8)\\ x\equiv a_{i,u_i}(\bmod p_i), i=1,2,\cdots,n,\\ x\equiv\alpha b_{j,v_j}(\bmod q_j), j=1,2,\cdots,m,\\ x\equiv\alpha e_t(\bmod r)\end{cases}$

has exactly one solution $x_{\alpha,\{u_i\},\{v_j\},t}$ modulo M .

It's obvious that $\left(x_{\alpha,\{u_i\},\{v_j\},t}, M\right)=1$ .By Lemma3,

$$\pi_r\left(x\right)=\sum_{\alpha\in\{\pm1\}}\sum_{u_1=1}^{\frac{p_1-1}{2}}\cdots\sum_{u_n=1}^{\frac{p_n-1}{2}}\sum_{v_1=1}^{\frac{q_1-1}{2}}\cdots\sum_{v_m=1}^{\frac{q_m-1}{2}}\sum_{t=1}^{\frac{r-1}{2}}\pi\left(x;M,x_{\alpha,\{u_i\},\{v_j\},t}\right)$$

$$\sim\sum_{\alpha\in\{\pm1\}}\sum_{u_1=1}^{\frac{p_1-1}{2}}\cdots\sum_{u_n=1}^{\frac{p_n-1}{2}}\sum_{v_1=1}^{\frac{q_1-1}{2}}\cdots\sum_{v_m=1}^{\frac{q_m-1}{2}}\sum_{t=1}^{\frac{r-1}{2}}\frac{\pi\left(x\right)}{\varphi\left(M\right)}$$

$$=2\cdot(\prod_{i=1}^{n}\frac{p_i-1}{2})(\prod_{j=1}^{m}\frac{q_j-1}{2})\cdot\frac{r-1}{2}\cdot\frac{\pi\left(x\right)}{\varphi\left(M\right)}$$

$$=\frac{\pi\left(x\right)}{2^{n+m+2}}=\frac{\pi\left(x\right)}{2^{\pi(r)}}\left(x\to\infty\right)$$

Therefore, Theorem 1 has been proved.

The proof of Theorem 2:

By Lemma 5 and Lemma 6, for $n>41$, there is k ,$1\le k\le n-1$, to make $g_n\left(k\right)$ composite.

If $1\le k<\frac{1}{2}+\sqrt{\frac{n}{3}}$, we need no further demonstration.

If $\frac{1}{2}+\sqrt{\frac{n}{3}}\le k\le n-1$,let r be the smallest prime factor of $g_n\left(k\right)$,

Then $r\le\sqrt{k^2-k+n}<n$ and $r\le\sqrt{k^2-k+3\left(k-\frac{1}{2}\right)^2}<2k-1$.

1° If $r<k$, let $k'=k-r$,thus $1\le k'<k$, $g_n\left(k'\right)=g_n\left(k-r\right)\equiv g_n\left(k\right)\equiv0\left(\operatorname{mod} r\right)$.

Also, $g_n\left(k'\right)\ge n>r$, hence $g_n\left(k'\right)$ is a composite number.

2° If $k\le r<2k-1$, let $k'=r+1-k$,thus $1\le k'<k$,

$g_n\left(k'\right)=g_n\left(r+1-k\right)\equiv g_n\left(1-k\right)=g_n\left(k\right)\equiv0\left(\operatorname{mod} r\right)$.

Also, $g_n\left(k'\right)\ge n>r$, hence is a composite number.

Therefore, for k with $\frac{1}{2}+\sqrt{\frac{n}{3}}\le k\le n-1$ and $g_n\left(k\right)$ a composite number, we are always able to find k', $1 \le k' < k$,to make $g_n(k')$ also a composite number. Repeat this procedure, we can eventually obtain k_0, $1 \le k_0 < \frac{1}{2} + \sqrt{\frac{n}{3}}$, to make $g_n(k_0)$ a composite number.

From the above mentioned, Theorem 2 has been proved.

The proof of Theorem 3:

(1)For $p \equiv \pm 1 (\bmod 8)$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$,hence $f(p) = 2 < \sqrt{p}$.

(2)For $p \equiv 5 (\bmod 8)$, by Lemma 4, p can be expressed as $p = x^2 + y^2$ with *x* and *y* positive integers.Suppose x is even, y is odd.

If $y = 1$, then $\frac{x^2}{4} = \frac{p-1}{4}$ is an odd number larger than 1. Let prime q divides $\frac{x}{2}$ exactly.

By Lemma 1, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{x^2+1}{q}\right) = 1$.Hence $f(p) \le q \le \frac{x}{2} < \sqrt{p}$.

If $y > 1$, let prime q divides y exactly.

By Lemma 1, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{x^2+y^2}{q}\right) = 1$.Hence $f(p) \le q \le y < \sqrt{p}$

(3)For $p \equiv 3 (\bmod 8)$, and $p > 163$, let $n = \frac{p+1}{4}$,then $n > 41$ and n is odd.

By Theorem 2, we can find k_0 ,$1 \le k_0 < \frac{1}{2} + \sqrt{\frac{p+1}{12}}$, to make $g_{\frac{p+1}{4}}(k_0)$ composite.

Let q be the smallest prime factor of the odd number $g_{\frac{p+1}{4}}(k_0)$, thus q divides $\frac{(2k_0-1)^2+p}{4}$ exactly.

By Lemma 1, $\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{-p}{q}\right) = \left(\frac{(2k_0-1)^2}{q}\right) = 1$,

Also, we can obtain $q \le \sqrt{\frac{(2k_0-1)^2+p}{4}} < \sqrt{\frac{\frac{p+1}{3}+p}{4}} < \sqrt{p}$ .Hence $f(p) \le q < \sqrt{p}$.

From the above mentioned, it completes the proof of Theorem 3.

In the investigating processes, we deeply realized the complexity of prime problems. In the 3000 years of history, countless predecessors did researches on prime, no matter deep or superficial. However, only some scattered and fragmentary results have been achieved**.** Since 19th Century, a lot of burgeoning approaches have made number theory evolved greatly, and a series of problems have been tackled in unified methods, nevertheless, little has been in repute about the important function $x^2 - x + n$ used in this paper. As math lovers in the new century, we are looking forward to the unit of number theory.

Thanks: Thanks to Wang Xiao. He helped to check the validity of Theorem 3 within primes smaller than 100 million at the beginning of this research.
Thanks to Professor Yu Hongbing. He gave us some valuable proposals to this paper.

References

【1】 华罗庚.数论导引.科学出版社,1975.
【2】 潘承洞 潘承彪.代数数论.山东大学出版社,2001.