The Least Inert Prime in a Real Quadratic Field

Enrique Treviño

Palmetto Number Theory Series
December 4, 2010
An upperbound on the least inert prime in a real quadratic field

An integer $D$ is a fundamental discriminant if and only if either $D$ is squarefree, $D \neq 1$, and $D \equiv \left(\text{mod } 4\right)$ or $D = 4L$ with $L$ squarefree and $L \equiv 2, 3 \left(\text{mod } 4\right)$.

**Theorem (Granville, Mollin and Williams, 2000)**

*For any positive fundamental discriminant $D > 3705$, there is always at least one prime $p \leq \sqrt{D}/2$ such that the Kronecker symbol $(D/p) = -1$.***
The least inert prime in a real quadratic field
Character Sums
Explicit Character Sums
Proof of main theorem
Future Work

Theorem (ET, 2010)

For any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$. 
Elements of the Proof

- Use a computer to check the “small” cases. Granville, Mollin and Williams used the Manitoba Scalable Sieving Unit.

- Use analytic techniques to prove it for the “infinite case”, i.e. the very large $D$. The tool used by Granville et al. was the Pólya–Vinogradov inequality. I used a “smoothed” version of it.

- Use Pólya–Vinogradov plus a bit of clever computing to fill in the gap.
Manitoba Scalable Sieving Unit
Let $\chi$ be a Dirichlet character to the modulus $q > 1$. Let

$$S(\chi) = \max_{M,N} \left| \sum_{n=M+1}^{M+N} \chi(n) \right|$$

The Pólya–Vinogradov inequality (1918) states that there exists an absolute universal constant $c$ such that for any Dirichlet character $S(\chi) \leq c \sqrt{q} \log q$.

Under GRH, Montgomery and Vaughan showed that $S(\chi) \ll \sqrt{q} \log \log q$.

Paley showed in 1932 that there are infinitely many quadratic characters such that $S(\chi) \gg \sqrt{q} \log \log q$. 
Further results regarding Pólya–Vinogradov

Granville and Soundararajan showed that one can save a small power of $\log q$ in the Pólya–Vinogradov inequality. Goldmakher improved it to

**Theorem (Goldmakher, 2007)**

*For each fixed odd number $g > 1$, for $\chi \pmod{q}$ of order $g$,*

$$S(\chi) \ll_g \sqrt{q} (\log q)^{\Delta_g + o(1)}, \quad \Delta_g = \frac{g}{\pi} \sin \frac{\pi}{g}, \quad q \to \infty.$$  

Moreover, under GRH

$$S(\chi) \ll_g \sqrt{q} (\log \log q)^{\Delta_g + o(1)}.$$  

Furthermore, there exists an infinite family of characters $\chi \pmod{q}$ of order $g$ satisfying

$$S(\chi) \gg_{\epsilon, g} \sqrt{q} (\log \log q)^{\Delta_g - \epsilon}.$$
Asymptotic results on least inert primes in a real quadratic field

- Using the Pólya–Vinogradov, it easily follows that there exists a \( p \ll \sqrt{D} \log D \) such that \( \left( \frac{D}{p} \right) = -1 \).

- By using a little sieving, we can improve this result: For every \( \epsilon > 0 \), there exists a prime \( p \ll \epsilon D^{\frac{1}{2\sqrt{e}}+\epsilon} \) such that \( \left( \frac{D}{p} \right) = -1 \).

- Using the Burgess inequality and a little sieving, we get the best unconditional result we have now: For every \( \epsilon > 0 \), there exists a prime \( p \ll_{\epsilon} D^{\frac{1}{4\sqrt{e}}+\epsilon} \) such that \( \left( \frac{D}{p} \right) = -1 \).
Theorem (Burgess, 1962)

Let $\chi$ be a primitive character mod $q$ with $q > 1$, $r$ an integer and $\epsilon > 0$ a real number. Then

$$S(\chi) \ll_{\epsilon, r} N^{1 - \frac{1}{r}} q^{\frac{r+1}{4r^2}} + \epsilon$$

for $r = 2, 3$ and for any $r \geq 1$ if $q$ is cubefree, the implied constant depending only on $\epsilon$ and $r$. 
Explicit Pólya–Vinogradov

Theorem (Hildebrand, 1988)

For $\chi$ a primitive character to the modulus $q > 1$, we have

$$|S(\chi)| \leq \begin{cases} \left( \frac{2}{3\pi^2} + o(1) \right) \sqrt{q \log q}, & \chi \text{ even}, \\ \left( \frac{1}{3\pi} + o(1) \right) \sqrt{q \log q}, & \chi \text{ odd}. \end{cases}$$

Theorem (Pomerance, 2009)

For $\chi$ a primitive character to the modulus $q > 1$, we have

$$|S(\chi)| \leq \begin{cases} \frac{2}{\pi^2} \sqrt{q \log q} + \frac{4}{\pi^2} \sqrt{q \log \log q} + \frac{3}{2} \sqrt{q}, & \chi \text{ even}, \\ \frac{1}{2\pi} \sqrt{q \log q} + \frac{1}{\pi} \sqrt{q \log \log q} + \sqrt{q}, & \chi \text{ odd}. \end{cases}$$
Explicit Burgess

Theorem (Iwaniec-Kowalski-Friedlander)

Let \( \chi \) be a Dirichlet character mod \( p \) (a prime). Then for \( r \geq 2 \)

\[
|S_\chi(N)| \leq 30 \cdot N^{1 - \frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.
\]

Theorem (ET, 2009)

Let \( \chi \) be a Dirichlet character mod \( p \) (a prime). Then for \( r \geq 2 \) and \( p \geq 10^7 \).

\[
|S_\chi(N)| \leq 3 \cdot N^{1 - \frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.
\]

Note, the constant gets better for larger \( r \), for example for \( r = 3, 4, 5, 6 \) the constant is 2.376, 2.085, 1.909, 1.792 respectively.
The least inert prime in a real quadratic field
Character Sums
Explicit Character Sums
Proof of main theorem
Future Work

Quadratic Case for Burgess

Theorem (Booker, 2006)

Let \( p > 10^{20} \) be a prime number \( \equiv 1 \pmod{4} \), \( r \in \{2, \ldots, 15\} \) and \( 0 < M, N \leq 2\sqrt{p} \). Let \( \chi \) be a quadratic character \( \pmod{p} \). Then

\[
\left| \sum_{M \leq n < M+N} \chi(n) \right| \leq \alpha(r)p^{\frac{r+1}{4r^2}}(\log p + \beta(r))^{\frac{1}{2r}}N^{1-\frac{1}{r}}
\]

where \( \alpha(r), \beta(r) \) are given by

<table>
<thead>
<tr>
<th>( r )</th>
<th>( \alpha(r) )</th>
<th>( \beta(r) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.8221</td>
<td>8.9077</td>
</tr>
<tr>
<td>3</td>
<td>1.8000</td>
<td>5.3948</td>
</tr>
<tr>
<td>4</td>
<td>1.7263</td>
<td>3.6658</td>
</tr>
<tr>
<td>5</td>
<td>1.6526</td>
<td>2.5405</td>
</tr>
<tr>
<td>6</td>
<td>1.5892</td>
<td>1.7059</td>
</tr>
<tr>
<td>7</td>
<td>1.5363</td>
<td>1.0405</td>
</tr>
<tr>
<td>8</td>
<td>1.4921</td>
<td>0.4856</td>
</tr>
<tr>
<td>9</td>
<td>1.4548</td>
<td>0.0085</td>
</tr>
<tr>
<td>10</td>
<td>1.4231</td>
<td>-0.4106</td>
</tr>
<tr>
<td>11</td>
<td>1.3958</td>
<td>-0.7848</td>
</tr>
<tr>
<td>12</td>
<td>1.3721</td>
<td>-1.1232</td>
</tr>
<tr>
<td>13</td>
<td>1.3512</td>
<td>-1.4323</td>
</tr>
<tr>
<td>14</td>
<td>1.3328</td>
<td>-1.7169</td>
</tr>
<tr>
<td>15</td>
<td>1.3164</td>
<td>-1.9808</td>
</tr>
</tbody>
</table>
Norton showed that for every prime $p$, its least quadratic non-residue is $\leq 4.7p^{1/4}\log p$.

For computing class numbers of large discriminants. Booker, computed the class number of a 32-digit discriminant.

To prove a conjecture of Brizolis (Levin, Pomerance) that for every prime $p > 3$ there is a primitive root $g$ and an integer $x \in [1, p - 1]$ with $\log_g x = x$, that is, $g^x \equiv x \pmod{p}$. 
Let $M, N$ be real numbers with $0 < N \leq q$, then define $S^*(\chi)$ as follows:

$$S^*(\chi) = \max_{M,N} \left| \sum_{M \leq n \leq 2N} \chi(n) \left( 1 - \left| \frac{a - M}{N} - 1 \right| \right) \right|.$$ 

**Theorem (Levin, Pomerance, Soundararajan, 2009)**

Let $\chi$ be a primitive character to the modulus $q > 1$, and let $M, N$ be real numbers with $0 < N \leq q$, then

$$S^*(\chi) \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$
Let $\chi$ be a primitive character to the modulus $q > 1$, and let $M, N$ be real numbers with $0 < N \leq q$, then

$$S^\ast(\chi) \geq \frac{2}{\pi^2} \sqrt{q}.$$ 

Therefore, the order of magnitude of $S^\ast(\chi)$ is $\sqrt{q}$. 
A little background on the smoothed Pólya–Vinogradov

L.K. Hua had proved an equivalent statement for prime modulus and used it to give an upperbound for the least primitive root.

**Theorem (Hua, 1942)**

Let $p > 2$, $1 \leq A < (p - 1)/2$. Then, for each non-principal character, mod $p$, we have

$$
\frac{1}{A + 1} \left| \sum_{a=0}^{A} \sum_{n=A+1-a}^{A+1+a} \chi(n) \right| \leq \sqrt{p} - \frac{A + 1}{\sqrt{p}}.
$$
Recall that we are dealing with $D$ a fundamental discriminant, i.e. either $D = L$ or $D = 4L$ where $L$ is squarefree. We only need to consider the cases $D \equiv 1 \pmod{8}$ and $D \equiv 2, 3 \pmod{4}$ because $D/2) = -1$ for $D \equiv 5 \pmod{8}$.

Running the Manitoba Scalable Sieving Unit (MSSU) for about 5 months yielded, among other things, the following information: If

1. $L \equiv 1 \pmod{8}$ with $(L/q) = 0$ or $1$ for all odd $q \leq 257$,
2. $L \equiv 2 \pmod{4}$ with $(L/q) = 0$ or $1$ for all odd $q \leq 283$ or
3. $L \equiv 3 \pmod{4}$ with $(L/q) = 0$ or $1$ for all odd $q \leq 277$

then $L > 2.6 \times 10^{17}$. 

Enrique Treviño
Counterexamples

The MSSU then allows us to know that we need only check up to $4(283)^2 = 320356$ for counterexamples below $2.6 \times 10^{17}$ (or $4 \times 2.6 \times 10^{17}$ in the case of $D$ even), for least inert primes $> \sqrt{D}/2$. The set of counterexamples is

$$S = \{5, 8, 12, 13, 17, 24, 28, 33, 40, 57, 60, 73, 76, 88, 97, 105, 120, 124,$

$$129, 136, 145, 156, 184, 204, 249, 280, 316, 345, 364, 385, 424, 456,$

$$520, 561, 609, 616, 924, 940, 984, 1065, 1596, 2044, 3705\}.$$

Similarly for the counterexamples to least inert prime $> D^{0.45}$, we need only check up to $283^{1/0.45} = 280811$. The set of counterexamples is

$$S' = \{8, 12, 24, 28, 33, 40, 60, 105, 120, 156, 184, 204, 280, 364, 456, 520, 1596\}.$$
Theorem (ET, 2010)

Let $\chi$ be a primitive character to the modulus $q > 1$, let $M, N$ be real numbers with $0 < N \leq q$. Then

$$\left| \sum_{M \leq n \leq M+2N} \chi(n) \left( 1 - \left| \frac{n - M}{N} - 1 \right| \right) \right| \leq \frac{\phi(q)}{q} \sqrt{q} + 2^{\omega(q)-1} \frac{N}{\sqrt{q}}.$$
Applying smoothed PV to the infinite case

Let $\chi(p) = \left( \frac{D}{p} \right)$. Since $D$ is a fundamental discriminant, $\chi$ is a primitive character of modulus $D$. Consider

$$S_{\chi}(N) = \sum_{n \leq 2N} \chi(n) \left( 1 - \left| \frac{n}{N} - 1 \right| \right).$$

By smoothed PV, we have

$$|S_{\chi}(N)| \leq \frac{\phi(D)}{D} \sqrt{D} + 2^{\omega(D)-1} \frac{N}{\sqrt{D}}.$$

Enrique Treviño

The Least Inert Prime in a Real Quadratic Field
Now,

\[ S_\chi(N) = \sum_{\substack{n \leq 2N \\ (n,D) = 1}} \left( 1 - \left| \frac{n}{N} - 1 \right| \right) - 2 \sum_{\substack{B < p \leq 2N \\ \chi(p) = -1}} \sum_{\substack{n \leq \frac{2N}{p} \\ (n,D) = 1}} \left( 1 - \left| \frac{np}{N} - 1 \right| \right). \]

Therefore,

\[ \frac{\phi(D)}{D} \sqrt{D} + 2^{\omega(D)} - 1 \frac{N}{\sqrt{D}} \geq |S_\chi(N)| \geq \frac{\phi(D)}{D} N - 2^{\omega(D)} - 2 \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D) = 1}} \sum_{\substack{B < p \leq \frac{2N}{n}}} \left( 1 - \left| \frac{np}{N} - 1 \right| \right). \]

Now, letting \( N = c\sqrt{D} \) for some constant \( c \) we get

\[ 0 \geq c - 1 - 2^{\omega(D)} \left( \frac{c}{2} + \frac{1}{4} \right) \frac{D}{\phi(D)\sqrt{D}} - \frac{2}{\sqrt{D}} \phi(D) \sum_{\substack{n \leq \frac{2N}{B} \\ (n,D) = 1}} \sum_{\substack{B < p \leq \frac{2N}{n}}} \left( 1 - \left| \frac{np}{N} - 1 \right| \right) \]
Eventually we have,

\[
0 \geq c - 1 - 2^{\omega(D)} \left( \frac{c}{2} + \frac{1}{4} \right) \frac{D}{\phi(D) \sqrt{D}} - \frac{2c}{\log B} e^{\gamma} \left( 1 + \frac{1}{\log^2 \left( \frac{2N}{B} \right)} \right) \log \left( \frac{2N}{B} \right) \prod_{\substack{p > \frac{2N}{B} \\ p \mid D}} \frac{p}{p - 1}.
\]

For \( D \geq 10^{24} \) this is a contradiction.
Hybrid Case

We have as in the previous case

\[ 0 \geq c - 1 - 2^{\omega(D)} \left( \frac{c}{2} + \frac{1}{4} \right) \frac{D}{\varphi(D) \sqrt{D}} - \frac{2}{\sqrt{D}} \frac{D}{\varphi(D)} \sum_{n \leq \frac{2N}{B}} \sum_{B < p \leq \frac{2N}{n}} \left( 1 - \left| \frac{np}{N} - 1 \right| \right) \]

In this case, since we don’t have to worry about the infinite case, we can have a messier version of

\[ \sum_{B < p \leq \frac{2N}{n}} \left( 1 - \left| \frac{np}{N} - 1 \right| \right). \]

The idea is to consider \(2^{13}\) cases, one for each possible value of \((D, M)\) where \(M = \prod_{p \leq 41} p\).
We consider the odd values and the even values separately. For odd values, the strategy of checking all the cases proves the theorem for $21853026051351495 = 2.2 \ldots \times 10^{16}$.

For even values we get the theorem for $1707159924755154870 = 1.71 \ldots \times 10^{18}$.

Here we need a little extra work, we find that there are 12 outstanding cases and we deal with them one at a time.

QED.
Future Work

- Bringing the upperbound further down.
- Generalizing to $D$’s not necessarily fundamental discriminants.
- Generalizing to other characters, not just the Kronecker symbol.
- Extending the explicit Burgess results to other modulus, not just prime modulus.
Acknowledgements

- My advisor Carl Pomerance for his guidance.
- Kannan Soundararajan for suggesting the problem to Carl.
- Bach, Booker, Burgess, Friedlander, Goldmakher, Granville, Hildebrand, Hua, Iwaniec, KIKSPC, Kowalski, Levin, MSSU, Mollin, Montgomery, Norton, Paley, Pólya, Pomerance, Soundararajan, Vaughan, Vinogradov and Williams for their work on character sums.