The least quadratic non-residue and related problems

Enrique Treviño

Swarthmore College

March 1st, 2011

Modular Arithmetic

In 7 hours it will be $11:30$ pm, in 8 hours it will be $12:30$ am, but in 9 it will be $1:30$ am.

- $4+7=11$
- $4+8=12$
- $4+9=1$

- $4+9 \equiv 1 \pmod{12}$
- $a \equiv b \pmod{n}$

Modular Arithmetic

In 7 hours it will be $11:30$ pm, in 8 hours it will be $12:30$ am, but in 9 it will be $1:30$ am.

- $4+7=11$
- $4+8=12$
- $4+9=1$

- $4+9 \equiv 1 \pmod{12}$
- $a \equiv b \pmod{n}$

Modular Arithmetic

In 7 hours it will be $11:30$ pm, in 8 hours it will be $12:30$ am, but in 9 it will be $1:30$ am.

- $4+7=11$
- $4+8=12$
- $4+9=1$

- $4+9\equiv 1 \pmod{12}$
- $a\equiv b \pmod{n}$

Modular Arithmetic

In 7 hours it will be $11:30$ pm, in 8 hours it will be $12:30$ am, but in 9 it will be $1:30$ am.

- $4+7=11$
- $4+8=12$
- $4+9=1$
- $4+9 \equiv 1 \pmod{12}$
- $a \equiv b \pmod{n}$

Modular Arithmetic

In 7 hours it will be $11:30$ pm, in 8 hours it will be $12:30$ am, but in 9 it will be $1:30$ am.

- $4+7=11$
- $4+8=12$
- $4+9=1$

- $4+9 \equiv 1 \pmod{12}$
- $a \equiv b \pmod{n}$

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod{7}$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod{7}$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Einstein's Birthday

Albert Einstein was born on March 14, 1879.

- 132 years ago, hence $132 \times 365 = 48180$ days.
- $132/4 = 33$ "leap years", hence 33 more days.
- 1900 was not a "leap year" hence -1 day.
- $14 - 1$ days between March 14 and March 1, so -13 days.
- Total Days Ago:
  $48180 + 33 - 1 - 13 = 48199 \equiv 4 \pmod 7$.
- Since today is Tuesday, four days ago it was Friday, so Einstein was born on a Friday.
- $365 \times 132 + 33 - 1 - 13 \equiv 1 \times 6 + 19 = 25 \equiv 4 \pmod 7$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0, 1 \text{ or } 2 \pmod 3$.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0$, 1 or 2 $\pmod 3$.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0, 1 \text{ or } 2 \pmod 3$.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0, 1 \text{ or } 2 \pmod 3$.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares

Consider the sequence

$$2, 5, 8, 11, \ldots$$

Can it contain any squares?

- Every positive integer n falls in one of three categories: $n \equiv 0$, 1 or 2 $\pmod 3$.
- If $n \equiv 0 \pmod 3$, then $n^2 \equiv 0^2 = 0 \pmod 3$.
- If $n \equiv 1 \pmod 3$, then $n^2 \equiv 1^2 = 1 \pmod 3$.
- If $n \equiv 2 \pmod 3$, then $n^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$.

Squares and non-squares

Let n be a positive integer. For $q \in \{0, 1, 2, \ldots, n-1\}$, we call q a square mod n if there exists an integer x such that $x^2 \equiv q \pmod{n}$. Otherwise we call q a non-square.

- For $n = 3$, the squares are $\{0, 1\}$ and the non-square is 2.
- For $n = 5$, the squares are $\{0, 1, 4\}$ and the non-squares are $\{2, 3\}$.
- For $n = 7$, the squares are $\{0, 1, 2, 4\}$ and the non-squares are $\{3, 5, 6\}$.
- For $n = p$, an odd prime, there are $\frac{p+1}{2}$ squares and $\frac{p-1}{2}$ non-squares.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Least non-square

How big can the least non-square be?

- For the least non-square to be > 2 we need 2 to be a square, therefore $p \equiv \pm 1 \pmod 8$, hence $p = 7$ is the first example.
- For the least non-square to be > 3 we need 2 and 3 to be squares, therefore $p \equiv \pm 1 \pmod 8$ and $p \equiv \pm 1 \pmod{12}$, therefore $p \equiv \pm 1 \pmod{24}$, giving us $p = 23$ as the first example.
- For the least non-square to be > 5 we need $2, 3$ and 5 to be squares, therefore $p \equiv \pm 1 \pmod 8$, $p \equiv \pm 1 \pmod{12}$ and $p \equiv \pm 1 \pmod 5$, therefore $p \equiv \pm 1, \pm 49 \pmod{120}$, giving us $p = 71$ as the first example.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log\log x$.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log\log x$.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log\log x$.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \le x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \le x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \le x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log \log x$.

Heuristics

Let $g(p)$ be the least non-square mod p. Let p_i be the i-th prime, i.e, $p_1 = 2, p_2 = 3, \ldots$.

- $\#\{p \leq x \mid g(p) = 2\} \approx \frac{x}{2}$.
- $\#\{p \leq x \mid g(p) = 3\} \approx \frac{x}{4}$.
- $\#\{p \leq x \mid g(p) = p_k\} \approx \frac{x}{2^k}$.
- If $k = \log x / \log 2$ you would expect only one prime satisfying $g(p) = p_k$, so if k is a bit bigger, then you wouldn't expect a prime with such a "large" least non-square.
- Then we want $k \approx C \log x$, and since $p_k \sim k \log k$ we have $g(x) \approx C \log x \log\log x$.

Theorems on the least non-square mod p

Let $g(p)$ be the least non-square mod p. Our conjecture is

$$g(p) = O(\log p \log\log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log\log\log p$, that is

$$g(p) = \Omega(\log p \log\log\log p).$$

Theorems on the least non-square mod p

Let $g(p)$ be the least non-square mod p. Our conjecture is

$$g(p) = O(\log p \log \log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log \log \log p$, that is

$$g(p) = \Omega(\log p \log \log \log p).$$

Theorems on the least non-square mod p

Let $g(p)$ be the least non-square mod p. Our conjecture is

$$g(p) = O(\log p \log\log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log\log\log p$, that is

$$g(p) = \Omega(\log p \log\log\log p).$$

Theorems on the least non-square mod p

Let $g(p)$ be the least non-square mod p. Our conjecture is

$$g(p) = O(\log p \log\log p).$$

- Under GRH, Bach showed $g(p) \leq 2\log^2 p$.
- Unconditionally, Burgess showed $g(p) \ll_\epsilon p^{\frac{1}{4\sqrt{e}}+\epsilon}$.
- $\frac{1}{4\sqrt{e}} \approx 0.151633$.
- In the lower bound direction, Graham and Ringrose proved that there are infinitely many p satisfying $g(p) \gg \log p \log\log\log p$, that is

$$g(p) = \Omega(\log p \log\log\log p).$$

Explicit estimates on the least non-square mod p

Norton showed

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET 2011)

Let $p > 3$ be a prime. Let $g(p)$ be the least non-square mod p. Then

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 1.2p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Explicit estimates on the least non-square mod p

Norton showed

$$g(p) \leq \begin{cases} 3.9p^{1/4}\log p & \text{if } p \equiv 1 \pmod 4, \\ 4.7p^{1/4}\log p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Theorem (ET 2011)

Let $p > 3$ be a prime. Let $g(p)$ be the least non-square mod p. *Then*

$$g(p) \leq \begin{cases} 0.9p^{1/4}\log p & \textit{if } p \equiv 1 \pmod 4, \\ 1.2p^{1/4}\log p & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

Quadratic fields and inert primes

- Let d be a squarefree integer.
- Then $\mathbb{Q}(\sqrt{d})$ is a quadratic field.
- A prime $p \in \mathbb{Z}$ is inert if it remains prime when it is lifted to the quadratic field.
- For example $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. In this field, the inert primes are the primes $p \equiv 3 \pmod 4$.
- Note that 5 is not prime in $\mathbb{Q}(i)$ because $(1+2i)(1-2i) = 5$. Similarly any prime $p \equiv 1 \pmod 4$ is not prime in $\mathbb{Q}(i)$ since p can be written as $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ and hence $p = (a+bi)(a-bi)$.

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square } \bmod p, \\ -1 & \text{if } a \text{ is a non-square } \bmod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square } \bmod p, \\ -1 & \text{if } a \text{ is a non-square } \bmod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

Characterization of inert primes in quadratic fields

- The discriminant D of a quadratic field $\mathbb{Q}(\sqrt{d})$ is d if $d \equiv 1 \pmod 4$ and $4d$ otherwise.
- A prime p is inert in $\mathbb{Q}(\sqrt{d})$ if and only if the Kronecker symbol $(D/p) = -1$.
- The Kronecker symbol is a generalization of the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square } \bmod p, \\ -1 & \text{if } a \text{ is a non-square } \bmod p, \\ 0 & \text{if } p \mid a. \end{cases}$$

The least inert prime in a real quadratic field

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 $(D/p) = -1$.

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 $(D/p) = -1$.

The least inert prime in a real quadratic field

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 $(D/p) = -1$.

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.

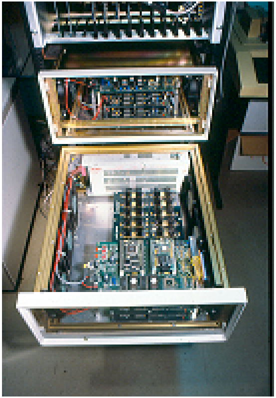
Elements of the Proof

- 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.

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



Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character $\bmod n$ if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ if and only if $\gcd(a, n) > 1$.

Examples of Dirichlet characters are the Legendre symbol and the Kronecker symbol.

Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod n if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ if and only if $\gcd(a, n) > 1$.

Examples of Dirichlet characters are the Legendre symbol and the Kronecker symbol.

Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod n if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ if and only if $\gcd(a, n) > 1$.

Examples of Dirichlet characters are the Legendre symbol and the Kronecker symbol.

Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod n if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ if and only if $\gcd(a, n) > 1$.

Examples of Dirichlet characters are the Legendre symbol and the Kronecker symbol.

Dirichlet Character

Let n be a positive integer.
$\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod n if the following three conditions are satisfied:

- $\chi(a+n) = \chi(a)$ for all $a \in \mathbb{Z}$.
- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$.
- $\chi(a) = 0$ if and only if $\gcd(a, n) > 1$.

Examples of Dirichlet characters are the Legendre symbol and the Kronecker symbol.

Pólya–Vinogradov

Let χ 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 $S(\chi) \gg \sqrt{q} \log\log q$.

Explicit Pólya–Vinogradov

Theorem (Hildebrand, 1988)

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

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

Theorem (Pomerance, 2009)

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

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

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{70}$.
- Levin and Pomerance proved a conjecture of Brizolis 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, $g^x \equiv x \pmod{p}$.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{70}$.
- Levin and Pomerance proved a conjecture of Brizolis 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, $g^x \equiv x \pmod{p}$.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{70}$.
- Levin and Pomerance proved a conjecture of Brizolis 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, $g^x \equiv x \pmod{p}$.

Some Applications of the Explicit Estimates

- The explicit estimate on the least quadratic non-residue showed earlier today.
- Booker computed the class number of a 32-digit discriminant using an explicit estimate of a character sum.
- McGown proved that there is no norm-Euclidean cubic field with discriminant $> 10^{70}$.
- Levin and Pomerance proved a conjecture of Brizolis 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, $g^x \equiv x \pmod{p}$.

Smoothed Pólya–Vinogradov

Let M, N be real numbers with $0 < N \leq q$, then define $S^*(\chi)$ as follows:

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

Theorem (Levin, Pomerance, Soundararajan, 2009)

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

$$S^*(\chi) \leq \sqrt{q} - \frac{N}{\sqrt{q}}.$$

Lower bound for the smoothed Pólya–Vinogradov

Theorem (ET, 2010)

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

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

Therefore, the order of magnitude of $S^*(\chi)$ is $\sqrt{q}$.

Tighter smoothed PV

Theorem (ET, 2010)

Let χ 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 least inert prime problem

Let $\chi(p) = \left(\frac{D}{p}\right)$. Since D is a fundamental discriminant, χ 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

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

Now,

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

- Therefore,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right).$$

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

$$0 \ge c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1-\left|\frac{np}{N}-1\right|\right)$$

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,

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

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

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

Now,

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

- Therefore,

$$\frac{\phi(D)}{D}\sqrt{D}+2^{\omega(D)-1}\frac{N}{\sqrt{D}} \ge \frac{\phi(D)}{D}N-2^{\omega(D)-2}-2\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right).$$

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

$$0 \ge c-1-2^{\omega(D)}\left(\frac{c}{2}+\frac{1}{4}\right)\frac{D}{\phi(D)\sqrt{D}}-\frac{2}{\sqrt{D}}\frac{D}{\phi(D)}\sum_{\substack{n\le \frac{2N}{B}\\(n,D)=1}} \sum_{B<p\le \frac{2N}{n}} \left(1 - \left|\frac{np}{N} - 1\right|\right)$$

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

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

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 $\gcd(D, M)$ 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 $218530260513514 95 = 2.2\ldots \times 10^{16}$.
- 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.

- 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.

- 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.

- 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 upper bound further down.
- Generalizing to D's not necessarily fundamental discriminants.
- Generalizing to other characters, not just the Kronecker symbol.
- Improving McGown's result on norm euclidean cubic fields.