Fake Real Quadratic Orders

Hongyan Wang

Supervised by: Renate Scheidler, Michael J. Jacobson, Jr.

hongyan.wang@ucalgary.ca

December 17, 2016

Motivation

- Proposed by Henry Cohen in 2013 [Coh13]
- FRQOs are defined based on imaginary quadratic fields but behave similarly to real quadratic orders
- Cohen-Lenstra Heuristics hold for real quadratic orders and FRQOs
- Ankeny-Artin-Chowla Conjecture does **NOT** hold for FRQOs

$$\Downarrow$$

NOT hold for real quadratic fields

Definition

Definition 1 [Coh13]

Let p be a fixed prime number. Take any fundamental discriminant $D < 0$ such that $(\frac{D}{p}) = 1$. We put $K = \mathbb{Q}(\sqrt{D})$ and let $\mathcal{O}_K$ denote its ring of integers. We write $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and define the ring $\mathcal{O}_K[\mathfrak{p}^{-1}]$ as a fake real quadratic order. Let $\mathcal{O}_{K,p}$ be the shorthand notation for it.

History

Cohen [Coh13]:

- Definition, theorems and numerical experiements
- Cohen-Lenstra Heuristics: experiments for $p < 30$ and $|D|$ up 2^{28}
- Ankeny-Artin-Chowla Conjecture: $p < 1000$ an $|D|$ up to 1072000

Oh [Oh14]:

- Proofs to all the theorems
- Mean number of three torsion elements

Contributions

- Repaired and clear proofs
- Description of infrastructure
- Cohen-Lenstra Heuristics:
  - Fixed p: $p = 2, 3, 5, 7, 11, 101, 1009$ and $|D|$ up 2^{40}
  - Fixed D: randomly selected D and p up to 30000
- Ankeny-Artin-Chowla Conjecture:
  - Counterexamples: $p = 2, 3, 5, 7, 11, 101, 1009$ and $|D|$ up to 2^{40}
  - Counterexamples: $D < 10 \cdot 2^{28}$ and p up to 30000
  - Counterexamples: selected large D, p up to 10^{11}
  - Proportion of Counterexamples: selected small D, p up to 10^{10}

Elements

Theorem 1 [Coh13]

Any element $\alpha \in \mathcal{O}_{K,p}$ can be written in a unique way as

$$\alpha = \frac{x + y\sqrt{D}}{p^k},$$

where $k \in \mathbb{Z}$, $x, y \in (\frac{1}{2})\mathbb{Z}$, $\gcd(x, y, p) = 1$, and either $k \leq 0$ (i.e. $\alpha \in \mathcal{O}_K$) or $k > 0$, which means that $\mathfrak{p}^k \mid x^2 - Dy^2$ and $x \equiv -sy \pmod{p}$ where $D \equiv s^2 \pmod{p}$.

Unit Group

Theorem 2 [Coh13]

Let $U_{K,p}$ denote the unit group of $\mathcal{O}_{K,p}$. Then $U_{K,p} = \mu_K \times \epsilon^{\mathbb{Z}}$, where μ_K is the group of roots of unity in $\mathcal{O}_K$, and the fundamental unit ϵ is a generator of the principal ideal $\mathfrak{p}^{o(\mathfrak{p})}$, where $o(\mathfrak{p})$ is the order of the class of $\mathfrak{p}$ in the ideal class group Cl_K.

Class Group

Theorem 3 [Coh13]

The class group $Cl_{K,p}$ of $\mathcal{O}_{K,p}$ is canonically isomorphic to $Cl_K / \langle [\mathfrak{p}] \rangle$, where Cl_K is the ideal class group of K and $\langle [\mathfrak{p}] \rangle$ is the cyclic subgroup of Cl_K generated by the class of $\mathfrak{p}$. In particular, we have $h_{K,p} = |Cl_{K,p}| = h_K / o(\mathfrak{p})$.

Computation

Resources:

- Class group tabulation for $|D|$ up to 2^{40} by Mosunov [Mos15]
- Implementation of ideal arithmetics by Sayles [Say13]

Servers:

- University of Calgary: Storm
- WestGrid: Breezy, Grex, Orcinus

Running time: 35 days

Cohen-Lenstra Heuristics

CL Heuristics for Real Quadratic Fields [CL84]

The proportion of real quadratic fields for which the odd part of the class number equals one should exist and be equal to

$$C = 1/\prod_{k\geq 2}(1-2^{-k})\zeta(k) = 0.754458173....$$

CL Heuristics for FRQOs

Let p be a prime number. Then the proportion of fake real quadratic orders for which the odd part of the class number equals one should exist and be equal to the constant $C = 0.754458173....$

Cohen-Lenstra Heuristics

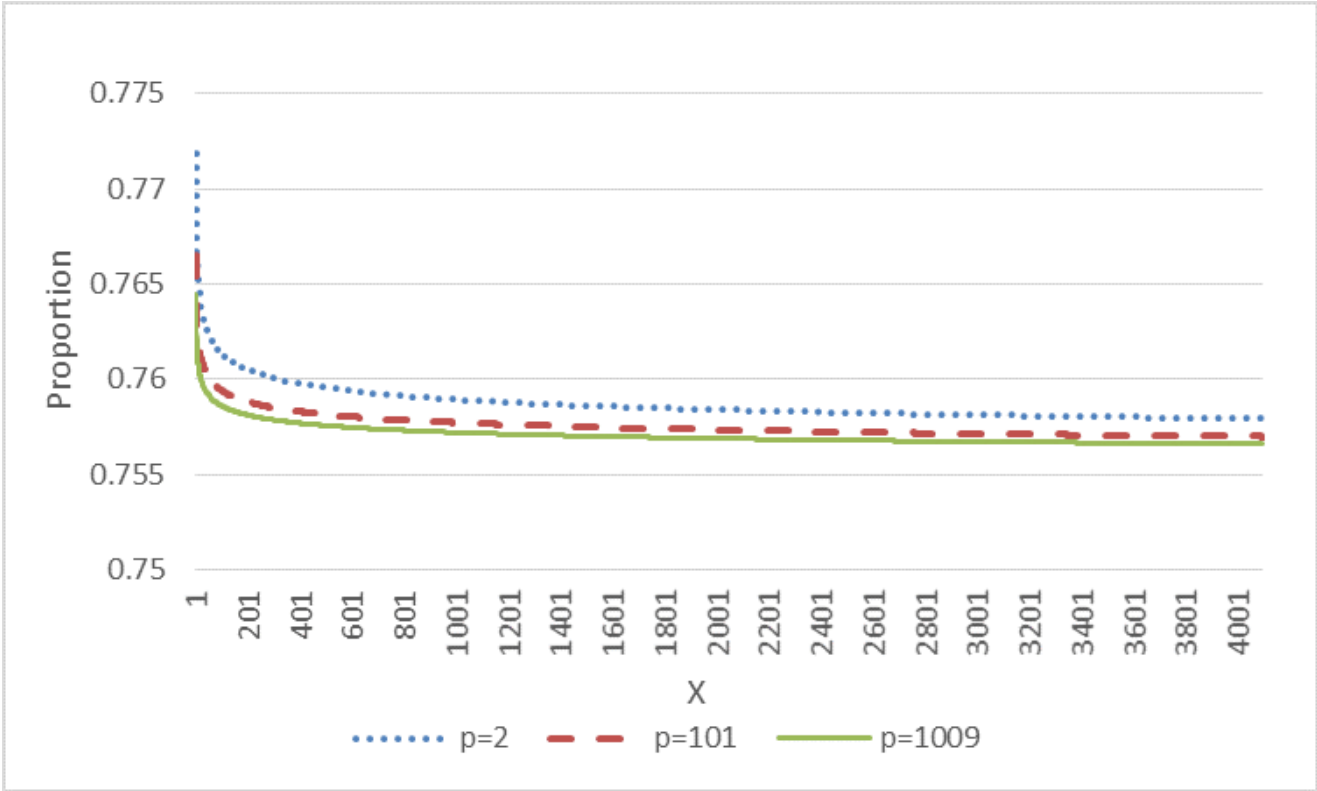

Figure: CL Heuristics for $p = 2, p = 101, p = 1009$, $|D|$ up to $X \cdot 2^{28}$

Ankeny-Artin-Chowla Conjecture

AAC Conjecture for Real Quadratic Fields [AAC52]

Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field where D is a prime discriminant such that $D \equiv 1 \pmod 4$ where the fundamental unit of K has the form $\epsilon = \frac{a+b\sqrt{D}}{2}$ with $a, b \in \mathbb{Z}$. Then $D \nmid b$.

*Note: No counterexamples have been found for D up to $2 \cdot 10^{11}$.
*The "log log" argument $\rightarrow$ The expected number of counterexamples for D up to $2 \cdot 10^{11}$ is no more than 1.4.

AAC Conjecture for FRQOs

Let $\epsilon = \frac{a+b\sqrt{D}}{2}$ be the fundamental unit of $\mathcal{O}_{K,p}$ with $a, b \in \mathbb{Z}$, where D is a prime discriminant. Then $D \nmid b$.

Counterexamples to the AAC Conjecture

- $D = -7,\ p = 29983,\ \epsilon = 164 + 21\sqrt{-7}$
- $D = -11,\ p = 29401,\ \epsilon = -325/2 - 33/2\sqrt{-11}$
- $D = -823,\ p = 21107,\ \epsilon = -642110 - 104521\sqrt{-823}$
- $D = -2147483647,\ p = 268435561,$
  $\epsilon = -165237779688422410874446106720082143507032972457555$
  $306387187269526286447109780559102312955058865108422004898$
  $16125105442037 9 - 64640734667080971294992512025395118428$
  $587383028721385469294340690007960750611541510969906683486$
  $4932578674749715716 60\sqrt{-2147483647}$

Counterexamples to the AAC Conjecture

- $D = -89716079$, $p = 11$, $\epsilon =$

$$\begin{aligned}
&3638777460537603923711326216762370699422558854080927147983442098897667636165187117224972351836137866209291903542432954299304715124943238060157080227241286509383904536940754667365474660368352757578234995047549158420275798021202989003985455116190513630725609219854461044064167501819157073496176461923908092792599094428983478003171870510894151383976289683796644475333704923714225057037137257354424642880232796551695973275699257908135668402101467303609668969604682011242688443187780551449518982813307831867866928526789692518284159955562618266543087671297419622737979993122987097236547585935569062874843867919337539645606354476946513317847622716745026992037126182708376567654254968053226547468269627336263156078889269870509190831038929870140456959307979256695136746538410094591457877603049410016260849536165479635316439481723661723339730934400238944963887071364540429734940860534911723360821086855598640422603734 - \\
&9454711281365024905609828622552157267447978905457095155877306710457026457257523800259152516324081166069524634383088039992542897888339155808190034162613715487646316154945369412612235917480093803939144946013539087339181287530249934014360822566690635928115376622008153039086467994592977296076640464030094901767856867492083275409624216022833538123110339496095653762979532105209495871415166931467185670236494083351144497166900737360561348627838810598528624093834367002376533931190281193868558702507272147436077535890456694308744289174304927733368239575439972112681204827441397030458580821482348957638314756457900894432667732553794193928927285176118626361450199136131832130821249537849284585188342248928151698250294387057862318177327838361256785427189237115371303063495329472845677626657172653209795502220168380204066151954868684585848931262639178728659942826617577292864921702890444244868426101869287335858951√−89716079
\end{aligned}$$

Proportions of Counterexamples to the AAC Conjecture

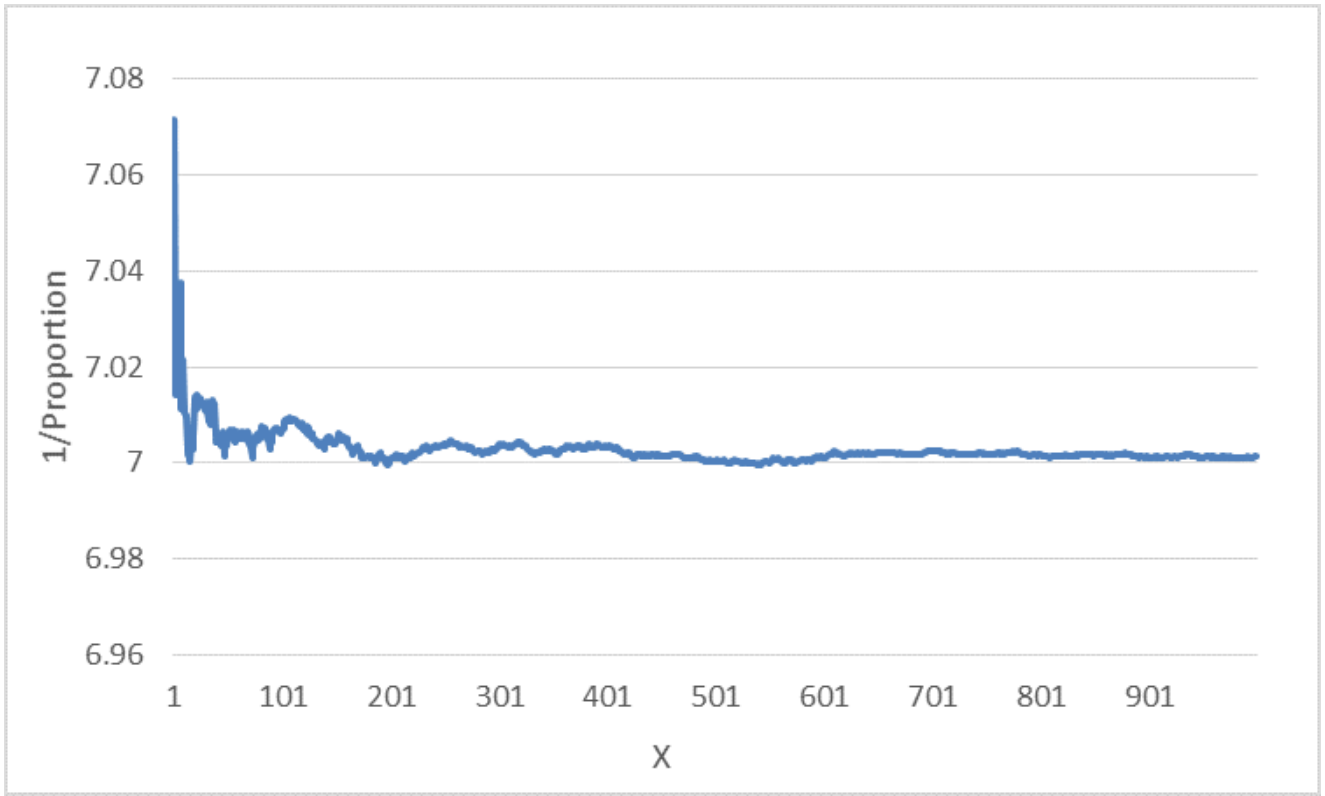

Figure: $D = -7$, p up to $X \cdot 10^7$

Proportions of Counterexamples to the AAC Conjecture

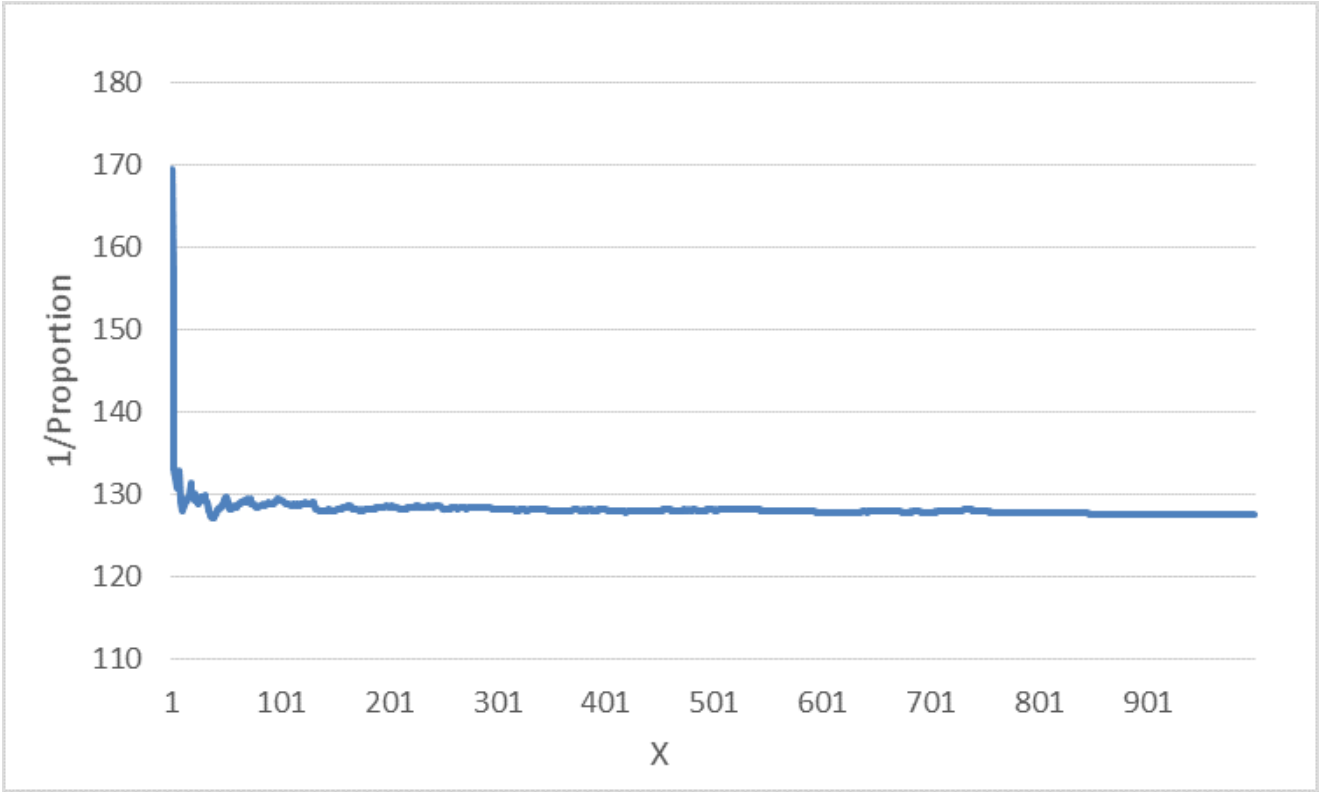

Figure: $D = -127$, p up to $X \cdot 10^7$

Proportions of Counterexamples to the AAC Conjecture

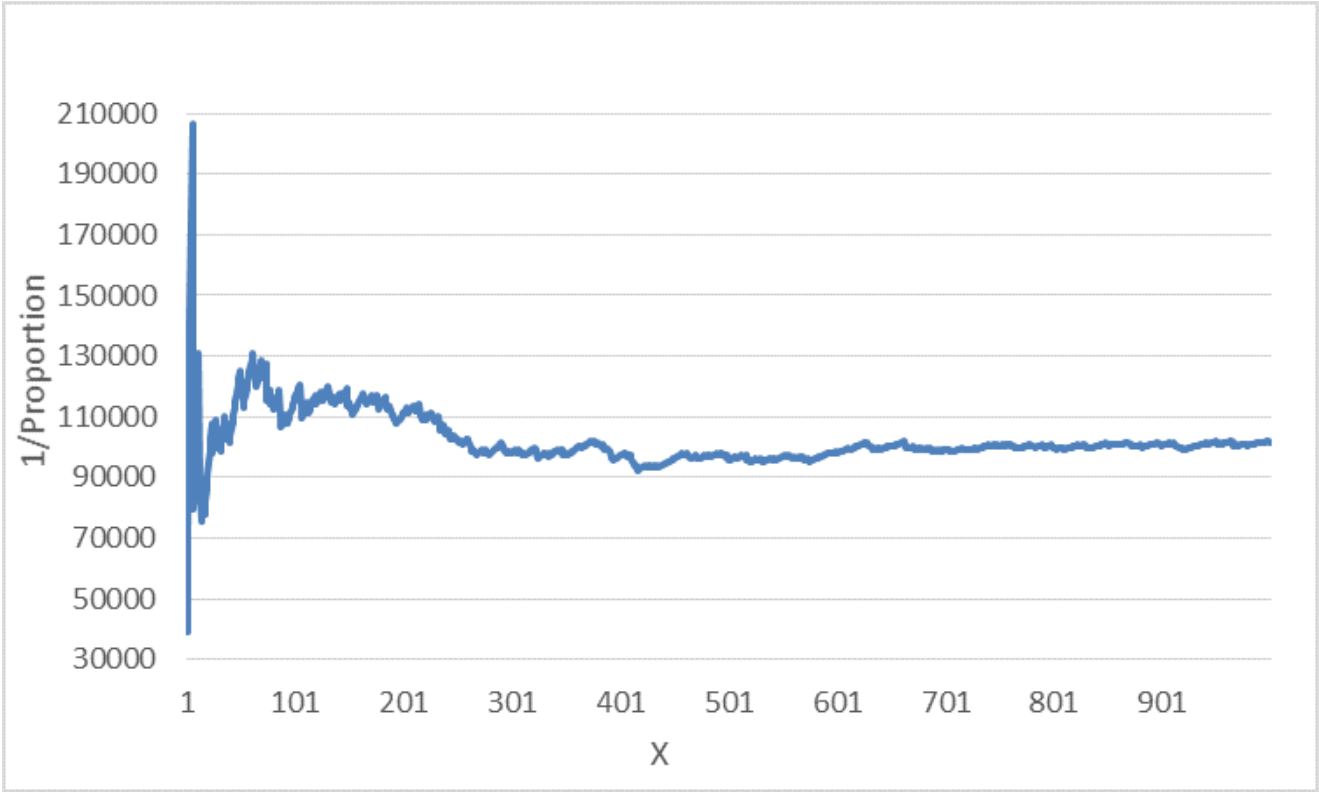

Figure: $D = -100019$, p up to $X \cdot 10^7$

Ankeny-Artin-Chowla Conjecture

The proportion of counterexamples converges to $1/|D|$ for any fixed D. Thus, the divisibility of b by D behaves randomly for any fake real quadratic order $\mathcal{O}_{K,p}$ with fundamental unit $\epsilon = \frac{a+b\sqrt{D}}{2}$.

We believe that the divisibility of b by D also behaves randomly for any real quadratic field $K = \mathbb{Q}(\sqrt{D})$ with fundamental unit $\epsilon = \frac{a+b\sqrt{D}}{2}$. Thus, the "log log" explanation is believed to be true.

Conjecture

The Ankeny-Artin-Chowla conjecture is false for real quadratic fields.

Conclusion

Cohen-Lenstra Heuristics:

- The probability of FRQOs for which the odd part of the class number equals $3, 5, 7...$
- The probability that any prime number q divides $h_{K,p}$ is equal to
$$1 - \prod_{k\geq 2}(1 - q^{-k}) = q^{-2} + q^{-3} + q^{-5} - q^{-7} - ...$$
where q
- The probability that the q-rank of $Cl_{K,p}$ equals r is $q^{-r(r+1)} \prod_{k\geq 1}(1 - q^{-k}) \prod_{1\leq k\leq r}(1 - q^{-k})^{-1} \prod_{1\leq k\leq r+1}(1 - q^{-k})^{-1}$

Ankeny-Artin-Chowla Conjecture:

- Experiments on larger discriminants with more prime numbers

References

Ankeny, Nesmith C. and Artin, Emil and Chowla, Sarvadaman D. S.(1952)

The class-number of real quadratic number fields

Ann. of Math. (2), 56:479–493.

Cohen, Henry and Lenstra, Jr., Hendrik W. (1984)

Heuristics on class groups of number fields

Number theory, Noordwijkerhout 1983, 1068:33–62.

Cohen, Henry (2013)

Experiments on fake real quadratic orders

Unpublished Manuscript.

Oh, Richard M. (2014)

Fake real quadratic orders

Doctoral Dissertation, University of South Carolina.

Mosunov, Anton S.(2015)

Unconditional class group tabulation of imaginary quadratic fields to 2^{40}

http://www.lmfdb.org/NumberField/QuadraticImaginaryClassGroups.

Sayles, Maxwell.(2013)

Implementation of ideal arithmetic in imaginary quadratic fields

https://github.com/maxwellsayles.

Thanks for your attention!