PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 17–21

Nathan Jones

The distribution of class groups of imaginary quadratic fields

written by Giulio Meleleo

The study of class groups and of class numbers has been a central task in number theory since their introduction, around 1845, by Kummer. The interest for the class group of imaginary quadratic fields goes actually back to Gauss, who in [2, art. 303-304], already predicted that there exists only finitely many imaginary quadratic number fields having a given class number and asked for a complete list of such number fields for each given value. Evidently Gauss formulated his result and conjecture in terms of quadratic forms. in 1934 Heilbron [3] established Gauss claim, by proving that the class number of imaginary quadratic number tends to infinity as the discriminant grows, and thus proving that every finite abelian group can appear as the class group of an imaginary quadratic field only finitely many times. It is then only natural to ask the following:

Question 1 *Let G be a finite abelian group. How many times does G occur as the class group of some imaginary quadratic field?*

Set

$$\mathcal{F}(G) := \#\{\text{imaginary quadratic fields } K \,:\, \mathrm{cl}(\mathcal{O}_K) \simeq G\}.$$

The following table is made out of a (much larger) set of data obtained by computations carried out with the aid of a supercomputer and under the GRH (cf. [4]):

p	3	5	7	11	13	17	19	23
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	33	93	130	241	335	518	599	823
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\times\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	1	2	2	0	5	1	0	1

Looking at the table it is natural to ask if $\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\times\frac{\mathbb{Z}}{p\mathbb{Z}}\right) > 0$ for infinitely many primes p. Evidently one can ask similar questions for groups of order p^n, for any $n \geq 2$. To formulate a precise question we need a little bit of notation. Let p be an odd prime. As it is well know isomorphism classes of abelian groups of order p^n are in one-to-one correspondence with the set of all possible partitions of n. Namely

$$\begin{aligned}\{[G] : G \text{ abelian group}, |G| = p^n\} &\leftrightarrow \mathrm{Part}(n)\\ \bigoplus_{i=1}^{k} \mathbb{Z}/p^{n_i}\mathbb{Z} &\mapsto (n_1, \ldots, n_k)\end{aligned}$$

where

$$\mathrm{Part}(n) = \left\{(n_1, \ldots, n_k) \in \mathbb{N}^k : \sum_{i=1}^{k} n_1{=}n,\ n_1{\geq}n_2{\geq}\cdots{\geq}n_k\right\}.$$

If $\lambda := (n_1, \ldots, n_k) \in \mathrm{Part}(n)$, we denote with $G_\lambda(p^n)$ the corresponding abelian group. Thus we can formulate the following

Question 2 *Is $\mathcal{F}\left(G_\lambda(p^n)\right) > 0$ for infinitely many primes p?*

Given $\lambda = (n_1, \ldots, n_k) \in \mathrm{Part}(n)$ let

$$\mathrm{cyc}(\lambda) := n_1 - \sum_{i=2}^{k}(2i-3)n_i.$$

Note that $1-(n-1)^2 \leq \mathrm{cyc}(\lambda) \leq n$ and is equal to n if and only if $G_\lambda(p^n)$ is cyclic.

Conjecture 3 (Holmin, Kurlberg, Jones, McLeman, Petersen) *Fix $n \in \mathbb{N}$ and $\lambda \in \mathrm{Part}(n)$. As $x \to \infty$, one has*

$$\sum_{p \leq x} \mathcal{F}(G_\lambda(p^n)) = \begin{cases} \frac{15C}{n(\mathrm{cyc}(\lambda)+1)} \cdot \frac{x^{\mathrm{cyc}(\lambda)+1}}{(\log x)^2}(1+o(1)) & \mathrm{cyc}(\lambda) \geq 0 \\ O(1) & \mathrm{cyc}(\lambda) < 0. \end{cases}$$

where C is defined by the Euler product

$$C := \prod_{\substack{\ell=3 \\ \ell \text{ prime}}}^{\infty} \prod_{i=2}^{\infty} \left(1 - \frac{1}{\ell^i}\right) \approx 0.754\ldots$$

It is interesting to see explicitly what the conjecture says for $n = 2, 3$.

$\boxed{n=2}$

Consider the partition $\lambda = (1,\ 1)$, for which $\mathrm{cyc}(1,\ 1) = 0$, we have the following set of data

p	3	5	7	11	13	17	19	23
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	1	2	2	0	5	1	0	1

The conjecture asserts that as $x \to \infty$,

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim \frac{15C}{2} \frac{x}{(\log x)^2}$$

In particular is expected that $\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) > 0$ for an infinite set of primes (of asymptotic density zero)

$\boxed{n=3}$

Consider the two partitions $(1,\ 2)$ ($\mathrm{cyc}(2,\ 1) = 1$) and $(1,\ 1,\ 1)$ ($\mathrm{cyc}(1,\ 1,\ 1) = -3$) , in this case the data collected in [4]) gives:

p	3	5	7	11	13	17	19
$\mathcal{F}\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	5	11	13	19	17	25	22
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	0	0	0	0	0	0	0

The conjecture asserts that as $x \to \infty$,

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim \frac{15C}{8} \frac{x^2}{(\log x)^2}$$

whereas

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim O(1)$$

The heuristic behind the conjecture is based on the Cohen-Lenstra heuristic for class groups (cf. [1]). Given G, set

$$P(G) := \frac{1/|\operatorname{Aut}(G)|}{\sum_{|H|=|G|} 1/|\operatorname{Aut}(H)|},$$

Then Cohen-Lenstra heuristic predicts that the probability of G being the class group of an imaginary quadratic field is exactly $P(G)$.

Let

$$\mathcal{F}(h) := \#\{\text{imaginary quadratic fields } K : |cl(\mathcal{O}_K)| = h\}.$$

So that $\mathcal{F}(h) = \sum_{|G|=h} \mathcal{F}(G)$, where the sum runs over the isomorphism classes of abelian groups of order h. By the Cohen-Lenstra heuristic one expects to have

$$\mathcal{F}(G_\lambda(p^n)) \approx P(G_\lambda(p^n)) \cdot \mathcal{F}(p^n).$$

In 1907, Ranum proved that for $\lambda \in \operatorname{Part}(n)$, one has $P(G_\lambda(p^n)) \sim p^{\operatorname{cyc}(\lambda)-n}$ for p that tends to infinity (see [5]). Moreover, a recent

conjecture of Soundararajan [6] says that for $h \to \infty$ through odd values, $\mathcal{F}(h) \asymp \frac{h}{\log h}$. Hence, we can deduce that

$$\mathcal{F}(G_\lambda(p^n)) \approx p^{\mathrm{cyc}(\lambda)-n} \cdot \frac{p^n}{\log(p^n)} = \frac{p^{\mathrm{cyc}(\lambda)}}{n \log p}.$$

Finally, we can see that

$$\sum_{p \le x} \mathcal{F}(G_\lambda(p^n)) \approx \sum_{p \le x} \frac{p^{\mathrm{cyc}(\lambda)}}{n \log p} \sim \frac{1}{n(\mathrm{cyc}(\lambda)+1)} \cdot \frac{x^{\mathrm{cyc}(\lambda)+1}}{(\log x)^2}.$$

This is, up to a the multiplicative constant $15C$ the content of Conjecture 3. The presence of $15C$ can be explained via the following refinement of Soundararajan's conjecture:

Conjecture 4 (Holmin, Kurlberg, Jones, McLeman, Petersen) *For $h \to \infty$ through odd values,*

$$\mathcal{F}(h) \sim 15 \cdot C \cdot c(h) \cdot \frac{h}{\log h}$$

where

$$c(h) = \prod_{p^n \,||\, h}^{\infty} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right)^{-1}$$

Another important theorem of Soundararajan [6] says that for $H \to \infty$, one has

$$\frac{1}{H} \sum_{h \le H} \mathcal{F}(h) \sim \frac{3\zeta(2)}{\zeta(3)} H.$$

A result related to this one is the following:

Theorem 5 (Holmin, Kurlberg, Jones, McLeman, Petersen) *Assume the Generalize Riemann Hypothesis. Then*

$$\frac{1}{H/2} \sum_{\substack{h \le H \\ h \ odd}} \mathcal{F}(h) \sim \frac{\pi^2 \zeta(2)}{\zeta(4)} \cdot \frac{H}{\log H}$$

for $H \to \infty$.

Lastly one can ask if a "typical" $G_\lambda(p^n)$ satisfies $\mathcal{F}(G_\lambda(p^n)) > 0$ infinitely often. An answer to this question is the following result.

Theorem 6 (Holmin, Kurlberg, Jones, McLeman, Petersen)

$$\frac{\#\{\lambda \in \mathrm{Part}(n) : \mathrm{cyc}(\lambda) \geq 0\}}{\#\,\mathrm{Part}(n)} \ll n^{5/4} e^{(2-\pi\sqrt{2/3})\sqrt{n}}.$$

In particular, almost all partitions $\lambda \in \mathrm{Part}(n)$ *conjecturally satisfy* $\mathcal{F}(G_\lambda(p^n)) = 0$ *for* $p \gg 1$.

The proof of this theorem is combinatorial, via generating functions.

For all the results highlighted in this extended abstract we refer the reader to [4].

References

[1] H. Cohen, and H.W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33-62

[2] C. F. Gauss, *Disiquisitiones Artithmeticae*, English Editon, Translated by Arthur A. Clarke, Springer-Verlag, New York, 1986.

[3] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields*, Quart. J. Math. Oxford Ser. 25, 150-160, 1934.

[4] S. Holmin, N. Jones, P. Kurlberg, P. McLeman, and K. Petersen, *Missing class groups and class number statistics for imaginary quadratic fields*, preprint.

[5] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. 8 (1907), 71–91.

[6] K. Soundararajan, *The number of imaginary quadratic fields with a given class number*, Hardy-Ramanujan J. 30 (2007), 13–18.

Giulio Meleleo
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146 Roma, Italy.
email: meleleo@mat.uniroma3.it