UNCONDITIONAL CLASS GROUP TABULATION TO $2^{40}$ FOR IMAGINARY QUADRATIC FIELDS

Anton Mosunov
University of Calgary
Alberta Mathematics Dialogue
May 1st, 2014
AGENDA

• Background
• Motivation
• Previous work
• Class number tabulation
• Out-of-core multiplication
• Results
• Future work
Consider a binary quadratic form \( ax^2 + bxy + cy^2 \) of discriminant \( \Delta = b^2 - 4ac < 0 \), \( a, b, c, x, y \in \mathbb{Z} \).

The substitution \( x = \alpha x' + \beta y', \ y = \gamma x' + \delta y' \) gives us another form \( a' x'^2 + b' x' y' + c' y'^2 \) of the same discriminant.

If \( \alpha \delta - \beta \gamma = 1 \), then the backward substitution exists. In that case, we call these two forms equivalent.
The set of all equivalent forms constitutes an equivalence class. The number of equivalence classes of a fixed discriminant $\Delta$ is always finite. It is called the class number, and usually denoted as $h(\Delta)$.

Example. $h(-15) = 2$. Every form of discriminant $\Delta = -15$ equivalent to one of the following two forms: $x^2 + xy + 4y^2$, $2x^2 + xy + 2y^2$. 
Furthermore, we can define an operation of composition $\circ$ under which the set of all equivalence classes forms a finite abelian group, i.e. $(a, b, c) \circ (a', b', c') = (a'', b'', c'')$

This group is called the class group, and denoted $Cl(\Delta)$.

Example. $h(-56) = h(-84) = 4$. However, $Cl(-56)$ has one generator $(3, 2, 5)$, and $Cl(-84)$ has two generators, $(5, 4, 5)$ and $(2, 2, 11)$.
GOAL

- Tabulate class numbers and class groups for every fundamental discriminant $|\Delta| < 2^{40}$. 
MOTIVATION

• Not much known about class groups.

• Want to provide an extensive computational evidence in support of the Cohen-Lenstra heuristics and the Littlewood’s bounds.

• Certain cryptosystems, such as the Buchmann-Williams key exchange protocol, rely on them. Want to have enough evidence that they hold.
PREVIOUS WORK

• In late 90s, Buell tabulated to $2.2 \times 10^9$, using algorithm for enumerating reduced forms. After computing all $h(\Delta)$, he produced $Cl(\Delta)$ by resolving structures of each p-group.

• In 2006, Ramachandran tabulated to $2 \times 10^{11}$ using Buchmann-Jacobson-Teske algorithm. The algorithm computes $Cl(\Delta)$ right away. However, it is conditional, and requires verification.

• We follow Buell’s approach. In order to compute all $h(\Delta)$, we use the algorithm due to Hart et al., who used an out-of-core polynomial multiplication technique to tabulate all congruent numbers to $10^{12}$. 
CLASS NUMBER TABULATION

- Let \( \nabla(q) = \sum_{n=0}^{\infty} q^{\frac{n(n+1)}{2}} = 1 + q + q^3 + q^6 + q^{10} + \ldots \)

\[ \psi_3(q) = 1 + 2 \sum_{n=0}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \ldots \]

- The following relations hold:

  (a) \[ \sum_{n=0}^{\infty} h(-16n - 4)q^n = \frac{1}{2} \nabla(q^2)\psi_3^2(q) \]

  (b) \[ \sum_{n=0}^{\infty} h(-16n - 8)q^n = \nabla^2(q^2)\psi_3(q) \]

  (c) \[ \sum_{n=0}^{\infty} h(-8n - 3)q^n = \frac{1}{3} \nabla^3(q) \]
CLASS NUMBER TABULATION

• Compute (a) and (b) to $2^{36}$, and (c) to $2^{37}$. This allows us to produce all $\Delta$, except $\Delta \equiv 1 \pmod{8}$.

• The following relations hold:

\[
\begin{align*}
(a) \quad \sum_{n=0}^{\infty} h(-16n - 4)q^n &= \frac{1}{2} \nabla(q^2)\vartheta_3^2(q) \\
(b) \quad \sum_{n=0}^{\infty} h(-16n - 8)q^n &= \nabla^2(q^2)\vartheta_3(q) \\
(c) \quad \sum_{n=0}^{\infty} h(-8n - 3)q^n &= \frac{1}{3} \nabla^3(q)
\end{align*}
\]
OUT-OF-CORE MULTIPLICATION

• We want to compute the product of two polynomials, $h(x) = f(x) \times g(x)$ each of length $2^{36}$. Each coefficient is of size 4 bytes, so in total we require at least

$$3 \cdot 4 \cdot 2^{36} \text{ bytes} = 768 \text{ Gb}$$

of memory.

• Need to store intermediate results on hard disk.

• Need multithreaded environment.

• For our computations, we utilize an out-of-core Fast Fourier Transform with Chinese Remainder Theorem (not trivial).
RESULTS

• We were using Westgrid’s Hungabee supercomputer.

• For each multiplication, we requested 64 processors with 8Gb of memory per core.

• (a) to $2^{36}$ terminated in 11 h 20 min (412.3 Gb)

• (b) to $2^{36}$ terminated in 10 h 25 min (395.1 Gb)

• (c) to $2^{37}$ terminated in 39 h 40 min (859 Gb)
RESULTS

• Ramachandran’s approach allows to compute class groups right away. However, we estimated that this approach would take at least 4 months. Moreover, the result is dependent on Extended Riemann Hypothesis, and requires an additional verification step.

• Out-of-core multiplication approach is unconditional, and allows to produce 2/3 of all class numbers to $2^{40}$ in 2.5 days!

• Now that we know class numbers, it is easier to compute class groups.
FUTURE WORK

• Tabulate class groups.

• Tabulate $\Delta \equiv 1 \pmod{8}$ with the Buchmann-Jacobson-Teske algorithm. These computations have to pass a verification procedure to be unconditional.

• Need to gather statistics to verify hypotheses.

• Challenge. Is there a better way of tabulating class numbers for discriminants $\Delta \equiv 1 \pmod{8}$ unconditionally?
THANK YOU VERY MUCH FOR YOUR ATTENTION