Travel Report from Kaliningrad

I attended a summer school in Kaliningrad, Russia titled "Euclidean Lattices – Theory and Application" from the July 15th to 19th. Because of vacation and planning issues, I could only attend the summer school from the 17th of July, but I think the stay was worthwhile anyway. There were about 30 participants at the summer school ranging from master's students to post-docs and industry people.

The School

We were located at Immanuel Kant Baltic Federal University. The days were organized with two double-hour lectures in the morning and exercises after lunch. The lectures were held by Prof. Alexander May and Prof. Damien Stehlé.

Alexander May lectured about the state-of-the-art of attacks on lattice-based crypto. In particular, he presented progressively better algorithms for solving the Shortest Vector Problem in a lattice. Personally, I had only seen these attacks vaguely, so getting a rigorous introduction to how vulnerable lattices are was very interesting.

In this cryptoanalysis we learned about how to solve problems using representations, that is, we saw algorithms using different representations of the input of a problem. This was very valuable because of the change in perspective of the problem being solved.

Damien Stehlé talked more generally about the theory of Euclidean lattices, lattice-primitives and hard problems in lattice-cryptography. This was more familiar to me, but nevertheless valuable. Among other things, we were introduced to the Learning With Errors and Short Integers Solution problem and saw a reduction between the two.

Towards the end of Stehlé's lectures, we also saw some constructions based on the LWE problem, most notably the signatures Scheme of Lyubashevsky.

On the 17th we went on an excursion to the Curonian Spit, a narrow, natural stretch of land from Kaliningrad Oblast to Lithuania. We visited a bird-sanctuary and a strange forest of twisty trees.

At the end of the last day there was a poster-session where some participants presented their ongoing and recently completed work. This ranged from hard-core algebra to using machine learning and coding theory to solve lattice-problems

The City

The whole Kaliningrad region became Russian in 1946 and was German before this. After it became Russian, many old, German churches and historical building were demolished and replaced by new ones. This gives the "historical" buildings of Kaliningrad a strange look, as they are clearly fairly new and too clean.

It is a beautiful city, and because of the history looks like a mix between a European city and a Russian city. It appeared to be a popular tourist destination for Russians.

The Kaliningrad region boasts 90% of the world's supply of amber and souvenir shops sells mostly amber trinkets. There was no shortage of these souvenir shops close to the city center.

Travel

Because Kaliningrad is such a small city, getting there was a bit difficult. My inbound flight had 1 stop, and my return flight had 3(!) stops.