Factoring Projects

by William Gasarch

Here is a list of projects and ideas for projects. They can also be combined.

1. Whatever you do with factoring you will need to code up the trivial algorithm so that you can compare the others ones to it.

2. In the first batch of slides I discuss how Golumb factored Jevon's Number. As stated, this was not an algorithm, it was just how to factor one number. Make it into an algorithm and compare to other algorithms.

3. Code up Pollard's algorithm. There are two versions, so you can compare them. The run time is $N^{1/4}$ though I suspect it is much better. Find out if this is true.

4. Code up Quadratic Sieve. This will be a massive undertaking and is best done by a set of programmers. Fine Tune the paramters. QS works well on large numbers (perhaps larger than we can deal with) but I speculate that with the right paramters it will work well even on smallish numbers. Compare to other algorithms and do some of the speedups suggested, and see if they speed it up.

5. The QS has many nuances to it. So when coding up keep track of what decisions you make and see if any make it faster.

6. The Number Field Sieve is an improvement on the QS. I have been wanting to learn it but have not. Perhaps we can learn it together.

7. All of the above are meant to be on numbers that are not that big. This is very educational purposes. My impression is that trying to get this to all work on actual large numbers is messy and not worth our efforst. Even so, if you have a way to do it, you can try. (Quadratic Sieve is especially troublesom)

8. All of the above can be combined with a crack-RSA project where you code up RSA and use the factoring algorithm to crack it. Again, this would only be with smallish numbers and for educational purposes.

9. If YOU come up with a factoring project, we can discuss it and I can help you with it.