

Some Possible Projects for the 2011 Computational Number Theory REU

Rose-Hulman Institute of Technology

June 8, 2011

All papers and code are linked from <http://www.rose-hulman.edu/~holden/REU/> unless otherwise noted. All books will be available in the REU number theory room.

Some of the papers are harder than others — that does not necessarily mean that the corresponding projects are harder. It's okay if you do not understand everything you read.

1. Complicated, but similar to things that have been done before:
 - (a) The quaternary (etc.) case
Start reading the papers by Brugger and Brugger & Frederick.
 - (b) Missing variances for the unary (permutation) case
Start reading the paper by Hoffman.
 - (c) Variances for the ternary case
Start reading the paper by Lindle.
 - (d) Statistical tests for the ternary case
Start reading the paper by Lindle.
 - (e) Distributions for the binary (and ternary) cases
Start reading the paper by Hoffman.
 - (f) More work on the “self-power” map $x \mapsto x^x \pmod p$
Start reading the paper by Friedrichsen, Larson, and McDowell.
 - (g) More work on elliptic curves
Start reading the paper by Blumenfeld.
 - (h) (Hard) Missing predictions in the ternary case
Start reading the paper by Cloutier & Holden.
 - (i) (Programming) Data collection for new parameters, e.g. average component size as seen from a node, maximum component size, average tree size as seen from a node, maximum tree size
Start looking at the code by Hoffman.

- (j) (Programming/Algorithms) Improving the graph theory algorithms for measuring parameters in the current code
Start looking at the code by Hoffman.
 - (k) The “square discrete exponentiation” map $x \mapsto g^{x^2} \bmod p$
We haven’t looked at this map yet, but see the paper by Cloutier & Holden for ideas of how we got started on the discrete exponentiation map.
2. Easy to get started but don’t know where it goes next:
- (a) Predictions for new parameters, e.g. average component size as seen from a node, maximum component size, average tree size as seen from a node, maximum tree size
Start reading the papers by Brugger and Brugger & Frederick
 - (b) The “discrete Lambert” map $x \mapsto xg^x \bmod p$
This map doesn’t seem to have gotten much attention, but see the paper by Friedrichsen, Larson, and McDowell for ideas on how a similar map was investigated.
 - (c) Combinatorial formulas for the binary (etc.) case
Start reading the sections on counting permutations and graphs in the book *Introduction to Enumerative Combinatorics* by Bóna or the books *Enumerative Combinatorics*, volumes 1 and 2, by Stanley, or the book *Concrete Mathematics*, by Graham, Knuth, and Patashnik.
 - (d) Prime power moduli
Start reading the paper by Mace.
 - (e) “Multi-maps” $x \bmod p^e \mapsto g^x \bmod p^e$ (or similar maps) for any x
Start reading the paper by Glebsky (not hard math but hard to read) and the paper by Holden & Robinson (vice versa?).
 - (f) Two-prime moduli
Start reading the paper by Mace.
 - (g) Finite fields
Start reading the paper by Odlyzko (“Discrete Logarithms in Finite Fields and Their Cryptographic Significance”). See also Section IV.3 of *A Course in Number Theory and Cryptography*, by Koblitz.
 - (h) Matrix groups
Start reading the paper by Sakalauskas, Listopadskis, and TvariJonas. Feel free to start on page 94 with the actual matrices.
 - (i) Discrepancies in the distribution of cycle lengths in the unary case (a little harder)
Start reading the papers by Hoffman and Holden & Moree (“Some heuristics and results for small cycles of the discrete logarithm”).

- (j) Using the observed discrepancies in the variances to break the Blum-Micali CSPRNG or a variation (maybe slowly)

Start reading the paper by Blum and Micali and looking at the code by Hoffman.

3. Need a new idea to get started:

- (a) Missing variances in the binary case

Start reading the paper by Cloutier & Holden.

- (b) Discrepancies in the variances in the unary and binary cases

Start reading the papers by Hoffman and Lindle.

- (c) Other groups

Start reading the paper by Lee, Kim, Kwon, Nahm, Kwak, and Baek. (Hard.)

Or come see me, especially if you have some other group in mind.

4. Think of your own possible projects

Please check with me to see if they seem reasonable!

In any case: Start/keep drawing graphs and making conjectures!