Review List for Math 788: Computational Number Theory*

1. Be able to do problems related to any of the homework. This includes homework problems not directly related to computational aspects of number theory such as topics in Elementary Number Theory and problems on notation. It also includes material not covered below (for example, public-key encryption). Look over practice problems.

2. Be able to prove that $\gcd(u, v)$ is $\asymp \log N$ on average and that usually it's much smaller.

3. Be able to define a strong pseudoprime to the base b and be able to prove that no n is a strong pseudoprime to every base b with $1 \le b \le n$ and $\gcd(b, n) = 1$.

4. Be able to check if a number is prime by using Maple's version of the Lucas-Lehmer test. (This is not a sure prime test.)

5. Be able to state and prove the Proth, Pocklington, Lehmer Test for primality.

6. Be able to prove that most numbers n have a prime factor $> \sqrt{n}$.

7. Be able to explain Pollard's ρ-Algorithm including Floyd's cycle-finding algorithm.

8. Be able to factor n using Dixon's Algorithm (see homework). (You will be given some information and you will need to make use of it and give the remaining details.)

9. Be able to factor n using the Quadratic Sieve Algorithm. (You will be given some information and you will need to make use of it and give the remaining details.)

10. Be able to prove Landau's inequality for the size of the factors of a polynomial.

11. Let $f(x) = \sum_{j=1}^{n-1} a_j x^j \in \mathbb{C}[x]$ and recall (7) from the notes which reads

$$D \langle a_0, a_1, \dots, a_{n-1} \rangle^T = \langle f(1), f(\omega), \dots, f(\omega^{n-1}) \rangle^T.$$

Show that the right side can be computed in $\ll n \log n$ total arithmetic operations (additions, subtractions, multiplications or/and additions).

12. Be able to state and prove Hadamard's inequality. (You do not need to be able to define the $\mathbf{b}_j^*$, but you should know that they are orthogonal and use this fact.)

13. Be able to define what it means for a basis in a lattice to be *reduced*.

14. Be able to show (10) in the notes, that is that

$$\mathbf{b} \in \mathcal{L},\ \mathbf{b} \neq \mathbf{0} \implies \|\mathbf{b}_1\| \le 2^{(n-1)/2} \|\mathbf{b}\|.$$

---

*You have the power to request and even make changes to the list above. I have the power to veto the changes.