Math 204A (Number Theory), UC San Diego, fall 2022
Problem Set 1 – due Thursday, October 6, 2022

Solutions should be submitted via CoCalc. To do this, place your solutions in the folder `assignments/2022-10-06/` in your course project. This folder acts like a homework dropbox; note that *all* files in the folder will be submitted, so please make it clear what I am supposed to be grading. If you have any trouble with this, PM me on Zulip for assistance.

You may submit handwritten text (scanned from paper or written on a tablet), a typed PDF (e.g., created using LaTeX on CoCalc), a Jupyter notebook, or any combination of the above. I will return feedback as a text file in the same folder.

Collaboration and research is fine, as long as you do the following.

- Try the problems yourself first!
- Write the solutions in your own words.
- Acknowledge all sources and collaborators.
- Include any SageMath code that you used.

I plan to be a bit flexible about deadlines, but please let me know *in advance* so that I know when to expect everything in.

For each assignment, submit *at most five* of the listed problems.

1. Fix a positive integer n.
   (a) Let P_n be the set of monic polynomials over $\mathbb{Z}$ of degree n, all of whose roots lie within the circle $|z| \leq 1$. Prove that P_n is finite. (Hint: use the Viète formulas.)
   (b) Let S_n be the subset of $\mathbb{C}$ consisting of the roots of the polynomials in P_n. Prove that S_n is closed under the map $z \mapsto z^2$. (Hint: for any given polynomial $f(x) \in P_n$, show that the polynomial whose roots are the squares of the roots of f also has coefficients in $\mathbb{Z}$.)
   (c) Deduce that every nonzero element of S_n is a root of unity. (This result is originally due to Kronecker.)
2. Neukirch, exercise I.2.4.
3. Do Neukirch, exercises I.2.5 and I.2.6 "by hand". Then use SageMath to confirm the result.
4. Examine the photo of my shower stall from fall 2020 (included in this folder). The black tiles correspond to primes in $\mathbb{Z}[\zeta_3]$. Identify at least five primes p of $\mathbb{Z}$ which do not remain prime in $\mathbb{Z}[\zeta_3]$, then for each p identify one tile in the photo corresponding to a prime lying over p.

5. For each of the following fields K, show that the ring of integers of K is Euclidean, and determine which rational primes factor nontrivially.

   (a) $\mathbb{Q}(\sqrt{-2})$, using the complex absolute value.

   (b) $\mathbb{Q}(\sqrt{-7})$, using the complex absolute value.

   (c) $\mathbb{Q}(\sqrt{2})$, using the function $a + b\sqrt{2} \mapsto |a^2 - 2b^2|$.

6. Neukirch, exercises I.3.1 and I.3.2.

7. Show that the ideal (2) in the ring $\mathbb{Z}[\sqrt{-3}]$ *cannot* be written as a product of prime ideals.

8. Write a subroutine in SageMath that implements Euclidean division with remainder for Gaussian integers (using SageMath's built-in class). Optional: use this to implement a gcd algorithm and check your work against SageMath's built-in function.