Elementary Number Theory: Review

Dr. Michael Woodbury

1. General guidelines

- Review all homework problems. Problems on the exam will be of the same basic nature. Many important ideas of the Skript are worked out and illucidated in the homework.
- Roughly 50% of the final exam will be proof/derivation based, and 50% will be computation/calculation based.
- You may bring a scientific calculator to the exam. No calculators will be allowed that can be programmed.
- In addition to the homework, the list of topics below is meant to be a review of the the main ideas of the Skript. I do not claim it to be all inclusive.

2. List of topics

- Division Algorithm: If $a, b \in \mathbb{Z}$ then there exists $q, r \in \mathbb{Z}$ such that $a = bq + r$ for some $r \in \mathbb{Z}$, $0 \leq r \leq |b|$. How does one prove this? What is the statement for a Euclidean domain generally?
- Definition: a divides b if there exists c such that $b = ac$. Notation: $a \mid b$. Properties? (See Satz 2.2 from the Skript for examples.) How does one prove these facts?
- Prime Numbers: Every $n \in \mathbb{N}$ has a decomposition as a product of primes. There are infinitely many primes. Given $n = p_1 \cdots p_r = q_1 \cdots q_s$ two prime decompositions of n, how does one prove that $r = s$ and the p's and q's are the same (with only possible reordering.) Main tool: If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$ which is proved using the Euclidean algorithm.
- Euclidean Algorithm: What is it? Why does it work? Important corollary (both theoretically and practically): $\{ax + by \mid x, y \in \mathbb{Z}\} = \{n \gcd(a, b) \mid n \in \mathbb{Z}\}$. Given one solution (x_0, y_0) to $ax + by = \gcd(a, b)$, how to find the rest?
- Irreducibility: in a general ring this is analogous to the notion of a prime number. Definition: $a \in R$ is irreducible if a is not a unit, and whenever

$a = bc$ then either b or c is a unit. Can any element be written as a product of irreducibles? If so, is this expression unique?

- Congruence modulo n: Definition, notation. Why are addition and multiplication well defined modulo n.
- Group theory: Axioms? Why is $(\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}, \times)$ a group if and only if p is prime? Euler's Theorem and proof. Fermat's Little Theorem.
- Pseudoprimes and Carmichael Numbers: if n is prime then $b^n \equiv b \pmod{n}$ for all $b \in \mathbb{Z}$. Is the reverse true?
- Chinese Remainder Theorem: Proof? How is it used? Application to determining values of the Euler φ-function.
- Method of Successive Squares. How does it work? How to use this find kth roots modulo n.
- Quadratic Reciprocity: What is the statement? Important steps leading to the proof:
  - Euler's Criterion: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$. How does the Primitive Element Theorem lead to the proof?
  - Primitive Element Theorem: $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. How does the fact that if k is a field then every $f \in k[x]$ has at most $\deg f$ roots and the characterization of cyclic groups lead to the proof?
  - Theorem that every $f \in k[x]$ has at most $\deg f$ roots.
  - Characterization of finite cyclic groups.
- Tonelli's Algorithm for finding a square root of a modulo p (assuming one exists).
- How to use quadratic reciprocity to prove the infinitude of primes congruent to 1 (or 3) modulo 4.
- Sums of squares and the Gaussian Integers. If p is prime then $p = a^2 + b^2$ if and only if $p \equiv 1 \pmod{4}$. Why? What about for nonprimes? How does the Euclidean algorithm work in $\mathbb{Z}[i]$?
- Continued Fractions.
  - To what extent are finite continued fraction expansions unique?
  - Infinite continued fraction expansions. What are the convergents $\frac{p_n}{q_n}$? What recursion relation do they satisfy? What does it mean for $[a_0, a_1, \ldots]$ to be *regular*? Does every regular continued fraction represent a real

number? (i.e. Do the sequence of convergents converge?) Does every real number have a representation by a regular continued fraction? If so, is this unique?

  - The continued fraction algorithm: if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ then $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha_0 \rfloor$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$ and $a_n = \lfloor \alpha_n \rfloor$. What recursion?

- Periodic Continued Fractions. Important fact: $\alpha_\ell = \alpha_j$ for some $j > \ell$ if and only if the continue fraction expansion of α is periodic. Why? Characterization of purely period continued fractions. What does this have to do with the continued fraction expansion of $\sqrt{d}$?

- Solutions to Pell's Equation. How to use the continued fraction expasion of $\sqrt{d}$ to find solutions to $x^2 - dy^2 = 1$.

- Approximation of real numbers by rationals. If $|x - \frac{a}{b}| < \frac{1}{2b^2}$ then $\frac{x}{y}$ is the convergent of the continued fraction expansion of x. This is used to show that if $x^2 + dy^2 = N$ for any $|N| < \sqrt{d}$, then $\frac{x}{y}$ comes from the continued fraction of $\sqrt{d}$. Liouville's theorem and its application to the existence of transcendental numbers.

- Elliptic Curves. Definitions, the point at infinity, the group law.