Key concepts:

1. Finite fields
2. Unique factorization
3. Fractional ideals and class groups

Reading List:

2. Next up: Marcus chapters 3-5.

Homework:

Do either problems (A)-(B) or problems (B)-(C). Due Fri 3/8.

Ireland-Rosen:
Chapter 7 (A) #6, 16 (B) #3, 15, (C) #17.
Chapter 13 (A) #1, 6, (B) #8, 18, (C) #19

Let \( \mathbb{F}_q \) denote the finite field of size \( q = p^a \). By FLT, \( \alpha^n = \alpha \) for all \( \alpha \in \mathbb{F}_q \).

1. If \( \alpha \in \mathbb{F}_q \), prove that the minimal polynomial \( f(x) \) for \( \alpha \) over \( \mathbb{F}_p \) divides \( x^a - x \).
2. Prove that \( \mathbb{F}_{p^a} \subset \mathbb{F}_{p^b} \) if and only if \( a \mid b \).
3. Hand in your data and observations about one of the SAGE problems.

Key concepts:

1. Integral bases
2. Quadratic reciprocity
3. Gauss sums

Reading List:

1. Ireland-Rosen, Sections 5.1-5.2, 6.2-6.3, 7.3.

Homework 3: Do either problems (A)-(B) or problems (B)-(C). Due Fri 2/22.

Ireland-Rosen:
Chapter 5: (A) #2, 4, 11, 16, (B) #7, 14, 15, (C) page 86 #7, 8
Chapter 6: (A) #9, 10, (B) #8, (C) #11
Key concepts:

1. Number fields and integral closure
2. The discriminant

Reading List: Try to read three of these references.

1. Marcus, Chapter 2.
2. Ogglier (short), Section 1.2.
3. Ireland-Rosen, Section 1.3-1.4, Section 12.1.

Theorem of the week: We will discuss this theorem on Monday 2/4.

1. Marcus, pages 11-12, Theorem 2 and Corollary 1.
2. Ogglier, page 9, Theorem 1.3 and Corollary 1.4.

Homework 2: Do either problems (A)-(B) or problems (B)-(C). Due Fri 2/8.
Marcus, Chapter 2: pages 28-38, (A) 1b, 7, 8b, 31 (B) 15, 16, 33, (C) 8ac, 35abcd.

Key concepts:

1. Quadratic fields and rings
2. Number fields and integral closure
3. Motivation from Fermat’s Last Theorem

Reading List: Try to read three of these references.

1. Marcus, Chapter 1, Chapter 2 pages 9-12.
2. Ogglier (short), Section 1.1.
3. Ireland-Rosen, Section 1.1-1.2 (E), Section 6.1.
**Theorem of the week:** We will discuss this theorem on Monday 1/28.

1. Marcus, pages 11-12, Theorem 2 and Corollary 1.
2. Ogglier, page 9, Theorem 1.3 and Corollary 1.4.

**Homework 1:** Do either problems (A)-(B) or problems (B)-(C). Due Wed 1/30.
Marcus, Chapter 1: pages 4-6, problems (A) 1-6, (B) 10,12,13, (C) 16,17,18.