Math 175: Elementary Number Theory

Syllabus: Week 3

Congruences and modular arithmetic

- Congruences classes modulo n
- $\mathbf{Z}/n\mathbf{Z}$ is a commutative ring
- $\mathbf{Z}/p\mathbf{Z}$ is a field
- Chinese remainder theorem: if $\gcd(a,b)=1$ then $\mathbf{Z}/ab\mathbf{Z} \simeq \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$
- Congruence equation: splitting principle
- Linear congruence equation
- Quadratic congruence equation in $\mathbf{Z}/p^n Z$ with $p \neq 2$
- Quadratic congruence equation in $\mathbf{Z}/p^n Z$ with $p = 2$
- Newton-Hensel method of solving congruence equation in $\mathbf{Z}/p^n\mathbf{Z}$