Math 175: Elementary Number Theory

Syllabus: Week 4

Invertible congruence classes

- $(\mathbf{Z}/n\mathbf{Z})^\times$ is an abelian group
- Euler totient function $\phi(n)$
- if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$
- Calculation of the totient function $\phi(p^r) = (p-1)p^{r-1}$
- Order of an element in an abelian group
- Euler-Fermat theorem
- Periods in decimal development of rational numbers
- $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic
- First criterion for an element in $(\mathbf{Z}/p\mathbf{Z})^\times$ to be a square
- Legendre symbol
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\mathbf{Z}/p^e\mathbf{Z}$ is cyclic for odd prime p
- $\mathbf{Z}/2^e\mathbf{Z}$ only for $e \leq 2$