Lectures 22 and 23

Summary

These lectures covered the applications of the multiplicative inverse in $\mathbb{Z}_n$, Fermat's Little Theorem, The Chinese Remainder Theorem, and and introduction to Encrypting and Encoding.

Little Fermat Theorem: If p is a prime, and $a \not\equiv 0 \bmod p$, then

$$a^{p-1} \equiv 1 \bmod p.$$

Chinese Remainder Theorem: If $\gcd(n, m) = 1$ and x satisfies the equations $x \equiv a \bmod n$ and $x \equiv b \bmod m$, then

$$x = b \cdot \lambda \cdot n + a \cdot \mu \cdot m$$

is the unique solution modulo nm with $1 = \lambda \cdot n + \mu \cdot m$.

Exercises on Lectures 22 and 23

1. Find $2^{200} \bmod 17$.
2. Find all x, with $-1000 \le x \le 1000$ such that $x \equiv 8 \bmod 25$. and $x \equiv 10 \bmod 32$.
3. Find 5^{500} modulo 2, 3, 4, 5, 6, 7, 8, 9, and 10.

   [In this problem, some of the cases you can do easily with Little Fermat, and others you can factor the modulus into two primes, solve those first and then put the solutions together with the Chinese Remember Theorem, and some, you to look for a pattern in the powers, like we did in class for $\mathbb{Z}_6$.]
4. Find 2^{1000} modulo 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 20.
5. Let the 26 letters of the alphabet be encoded in $\mathbb{Z}_{26}$ with a by 0, b by 1, etc. until z by 25. What is the encoding of *celtics*.