Lectures 17 and 18

We discussed the arithmetic of the systems $\mathbb{Z}_n$.

We illustrated the "Chinese Remainder Theorem" to solve

$$x \equiv b_1 \bmod n_1 \qquad x \equiv b_2 \bmod n_2 \qquad \gcd(n_1, m_1) = 1$$

Using $\lambda n_1 + \mu n_2 = 1$ as $x = b_2 \lambda n_1 + b_1 \mu n_2 = 1$.

We showed how to find the additive and multiplicative inverses in $\mathbb{Z}_n$. We showed that a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$, and how to use the multiplicative inverse to divide in $\mathbb{Z}_n$.

We discussed the multiplicative order in $\mathbb{Z}_n$ and showed that the multiplicative order of any element in $\mathbb{Z}_n$ divides the number of elements in $\mathbb{Z}_n$ which have multiplicative inverses.

In particular Fermat's Little Theorem: For any prime p and any $a \in \mathbb{Z}_p$ with $a \not\equiv 0 \bmod p$ satisfies $a^{p-1} \equiv 1 \bmod p$.

Exercises for Lectures 17 and 18

1. In $\mathbb{Z}_7$ compute the following. $15 + 25$, $15 - 25$, 15×25, $15 \div 25$,
2. In $\mathbb{Z}_{31}$ compute the following. $15 + 25$, $15 - 25$, 15×25, $15 \div 25$,
3. In $\mathbb{Z}_{101}$ compute the following. $15 + 25$, $15 - 25$, 15×25, $15 \div 25$,
4. In $\mathbb{Z}_{12}$ compute the following. $5 + 11$, $5 - 11$, 5×11, $5 \div 11$,
5. In $\mathbb{Z}_{24}$ find all elements which have multiplicative inverses, and find those inverses.
6. An band tries to march in rows of 8 but the last row has only 4 members. It is reorganized to march in rows of 11 but there are only 10 members. What is the fewest number of members this band can have?
7. Find an number which m such that $m \equiv 3 \bmod 5$, $m \equiv 5 \bmod 7$, and $m \equiv 7 \bmod 11$.
8. Find the multiplicative order of every non-zero element in $\mathbb{Z}_{17}$
9. Find the multiplicative order every element in $\mathbb{Z}_{30}$ which has multiplicative inverse. (There are eight of them.)
10. What are the possible multiplicative orders of elements in $\mathbb{Z}_{101}$?
11. Find an element of multiplicative order 2 in $\mathbb{Z}_{11}$?