Math 1560 - Notes 4

Ian Benway

10 February 2022

1 Congruence

Recall that for $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$, the linear congruence

$$ax \equiv b \mod m$$

has a solution if and only if $(a,m)|b$.
Q: How do we find a solution?
A: Either guess+check, or the following algorithm:

1. Divide all terms in the congruence by $d = (am)$.
2. If Step 1 yields

   $$a'x \equiv b' \mod m',$$

   with $(a',m') = 1$, then $d' := (a',b')$ is a unit mod m'. We can thus divide both sides by d' to get

   $$\frac{a'}{d'}x \equiv \frac{b'}{d'} \mod m'.$$

3. Let $a''x \equiv b'' \mod m'$ be the result so far. Replacing b'' by some $b'' + km'$ such that $(a'', b'' + km') > 1$ allows us to repeat Step 2. This results in some a''' such that $|a'''| < |a''|$.

Hence this process must terminate, because the absolute values of the a terms are strictly decreasing.

Example:

$$10x \equiv 6 \mod 14$$

Step 1: $5x \equiv 3 \mod 7$ since $(10,14) = 2$
Step 2: not important because $(5,3) = 1$
Step 3: Consider $3 + 7k$ and see which are divisible by 5. $k = 1$ works.
So $5x \equiv 10 \mod 7$. Divide by 5 on both sides to get $x \equiv 2 \mod 7$.

Simultaneous Linear Congruences

Recall Suzni's Theorem (Chinese Remainder Theorem):

Theorem 1 (Sunzi's Theorem)**.** *Suppose that $m = m_1 m_2 \dots m_k$ with $(m_i, m_j) = 1$. Let $b_1, b_2, \dots, b_k$ be integers, and consider the system of congruences*

$$\begin{aligned} x &\equiv b_1 \mod m_1 \\ x &\equiv b_2 \mod m_2 \\ &\vdots \\ x &\equiv b_k \mod m_k. \end{aligned}$$

Then this system has solutions, and they differ from each by a multiple of m.

Proof. Let $n_i = \frac{m}{m_i}$, for each i. Since m_i is coprime to m_j for all $j \neq i$, we have $(n_i, m_i) = 1$ for all i. Thus there exists $r_i, s_i \in \mathbb{Z}$ such that

$$r_i m_i + s_i n_i = 1.$$

Let $e_i = s_i n_i$. Then for each i,

$$\begin{aligned} e_i &\equiv 1 \mod m_i \\ \text{and} \quad e_i &\equiv 0 \mod m_j \quad \forall j \neq i. \end{aligned}$$

Our goal now is to show that $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, with each e_i generating the "$\mathbb{Z}/m_i\mathbb{Z}$ piece".

Set

$$x_o = \sum_{i=1}^{k} b_i e_i.$$

So that $x_o \equiv b_i (m_i)$ for all i, which is to say that x_o is a solution to the system of congruences above.
Suppose x_1 is another solution. Then

$$x_1 - x_o \equiv 0 \mod m_i \quad \forall i,\ 1 \leq i \leq k.$$

Since the m_i are pairwise coprime, we get $m | x_1 - x_o$. □

2 Structures of Unit Groups

Recall Lagrange's Theorem:

Theorem 2 (Lagrange's Theorem)**.** *If G is a finite group, then for every subgroup H of G, $|H| \,|\, |G|$ (i.e. the order of H divides the order of G).*

Corollary 1. *If G is a finite group of order n, and $a \in G$, then $a^n = e$, where e is the identity of the group.*

Let $U(m) := (\mathbb{Z}/m\mathbb{Z})^*$ be the group of units of $\mathbb{Z}/m\mathbb{Z}$. We've seen that $|U(m)| = \phi(m)$. Applying Lagrange's Theorem:

Theorem 3 (Euler's Theorem)**.** *For any $a \in \mathbb{Z}$ with $(a,m) = 1$, we have*

$$a^{\phi(m)} \equiv 1 \mod m.$$

Let's find an alternate proof to Euler's Theorem which doesn't need Lagrange's Theorem...

A subset R of $\mathbb{Z}$ is said to be a **reduced set of residues mod** m if R contains exactly one element from each of the $\phi(m)$ congruence classes that are units mod m.

Proof of Euler's Theorem without Lagrange. Let $R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced set of residues mod m. If $(a,m) = 1$, then aR is also a reduced set of residues mod m. Thus, if $x_1, x_2, \ldots, x_{\phi(m)} \in aR'$ are pairwise distinct, then $x_1 x_2 \ldots x_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \mod m$. Hence

$$\begin{aligned} (ar_1)(ar_2)\ldots(ar_{\phi(m)}) &\equiv r_1 r_2 \ldots r_{\phi(m)} \mod m \\ \Rightarrow a_{\phi(m)}(r_1 r_2 \ldots r_{\phi(m)}) &\equiv r_1 r_2 \ldots r_{\phi(m)} \mod m \\ \Rightarrow a^{\phi(m)} &\equiv 1 \mod m. \end{aligned}$$

□

We'll be studying roots of polynomials over $\mathbb{Z}/m\mathbb{Z}$, especially polynomials of the form $x^d - a$.
By Sunzi's Theorem, the case of m being a prime power is very important. This turns out to have a lot to do with the case when m is prime.

Proposition 1. *If p is a prime and $p \nmid d$, $d \in \mathbb{Z}_+$, then the polynomial*

$$x^d - a \in (\mathbb{Z}/p\mathbb{Z})[x], \qquad a \not\equiv 0 \mod p$$

has exactly d roots in some extension $\mathbb{F}_p$.
Conversely, if $p|d$, then there are fewer than d roots in any extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

The proof for this uses the following proposition:

Proposition 2. *A nonzero polynomial $f \in K[x]$ is separable if and only if it is relatively prime to f'. (A separable polynomial over K is one without repeated roots in $\bar{K}$.)*

Proof. ($\Rightarrow$) Suppose f is sepparable, and let α be any root of f. Then $f(x) = (x - \alpha)h(x)$, where $h(\alpha) \neq 0$. Have $f'(\alpha) = h(\alpha) \neq 0$, so α is not a root of f'. Thus, f and f' have no common roots, so they are coprime.

($\Leftarrow$) Suppose f is not separable, i.e., suppose f has some repeated root α. Then $f(x) = (x-\alpha)^2 g(x)$, so

$$f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x).$$

We see that $x-\alpha$ divides both f and f', so $(f, f') \neq 1$. □

Proof of Proposition 1. $f(x) = x^d - a$, $a \not\equiv 0 \mod p$ has d distinct solutions in some extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, because $f'(x) = dx^{d-1} \mod p$, and 0 is not a root of f. Conversely, if $p|d$, then $f'(x) \equiv 0 \mod p$. So, $(f, f') \neq 1$, meaning that f is not separable. □

Proposition 3. *If p is a prime, and if $d|p-1$, then the polynomial $x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has exactly d roots in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

Proof. We have $(x^d - 1)|(x^{p-1} - 1)$. So, if some root of $x^d - 1$ is <u>not</u> in $\mathbb{F}_p$, then some root of $x^{p-1} - 1$ is not in $\mathbb{F}_p$, contradicting Fermat's Little Theorem. □