Discrete Mathematics lecture notes 4-1

September 24, 2013

13. Solving linear equations in $\mathbb{Z}/n$

Last time we began consideration of modular number systems $\mathbb{Z}/n$, and observed that, unlike in $\mathbb{Z}$, a linear[1] polynomial can have multiple solutions. For example, in $\mathbb{Z}/12$, the linear equation $3x = 6$ has *three* solutions: $\{2, 6, 10\}$. We could find these solutions by checking, one at a time, whether each of the 12 elements of $\mathbb{Z}/2$ satisfies $3x = 6$: 0 doesn't, 1 doesn't, 2 does, 3 doesn't, ... This process will terminate, but what if we were working in $\mathbb{Z}/1024$, or something even more horrendous? We should have some more systematic method for solving these equations.

Let's start from the assumption that we have found *one* solution to $3x = 6$, say $x_0 = 2$.[2] If x_1 is any other solution, so $3x_1 = 6 = 3x_0$, then

$$0 = 3x_1 - 3x_0 = 3(x_1 - x_0)$$

If we were working in $\mathbb{N}$ or $\mathbb{Z}$, the equation $0 = 3(x_1 - x_0)$ would immediately imply that $x_1 - x_0 = 0$ (so $x_0 = x_1$), because the product of nonzero numbers is never zero.[3] However, in $\mathbb{Z}/12$, it is very easy to find nonzero numbers whose product is zero: 3 is a zero divisor in $\mathbb{Z}/12$. All that we've done here is show that if x_0 and x_1 are both solutions to $3x = 6$, then $x_1 - x_0$ is one of the numbers that annihilates 3:

Definition 1. The *annihilator* of a nonzero $a \in \mathbb{Z}/n$ is the set $\mathrm{Ann}(a) := \{b \in \mathbb{Z}/n | ab = 0\}$.

Note that the annihilator of a nonzero element is never empty, as $0 \in \mathrm{Ann}(a)$ for all $0 \neq a \in \mathbb{Z}/n$.

In $\mathbb{Z}/n$, the annihilator of a is easy to calculate using the Fundamental Theorem of Arithmetic: Let n have a prime factorization $n = \prod_{p \in \mathcal{P}} p^{\ell_p(n)}$ and a have prime factorization $a = \prod_{p \in \mathcal{P}} p^{\ell_p(a)}$.[4] If $b \neq 0$ is such that $ab = 0$ and $b = \prod_{p \in \mathcal{P}} p^{\ell_p(b)}$,[5] then

$$n | ab = \prod_{p \in \mathcal{P}} p^{\ell_p(a) + \ell_p(b)},$$

from which it follows that $\ell_p(n) \leq \ell_p(a) + \ell_p(b)$ for all $p \in \mathcal{P}$.

Proposition 2. *Given $n \in \mathbb{N}_{>0}$ and $a \in \{1, 2, \ldots, n-1\}$, set $m_p := \max\{\ell_p(n) - \ell_p(a), 0\}$.*[6] *Then*

$$\mathrm{Ann}(a) = \left\{ b \in \{1, 2, \ldots, n-1\} \middle| \ell_p(b) \geq m_p \ \forall\ p \in \mathcal{P} \right\} \cup \{0\}.$$

Proof. Exercise. □

For instance, in our situation comparing $n = 12$ and $a = 3$, we have

$$\ell_p(12) = \begin{cases} 2 & p = 2 \\ 1 & p = 1 \\ 0 & \text{else} \end{cases} \qquad \text{and} \qquad \ell_p(3) = \begin{cases} 1 & p = 1 \\ 0 & \text{else} \end{cases}, \qquad \text{so} \qquad m_p = \begin{cases} 2 & p = 2 \\ 0 & \text{else} \end{cases}$$

Therefore, if $b \in \mathrm{Ann}(3)$, we must have $\ell_2(b) \geq 2$, or $4|b$, so $\mathrm{Ann}(3) = \{0, 4, 8\}$.

Returning to our original problem: Now that we've found the annihilator of 3 in $\mathbb{Z}/12$ and a particular solution to $3x = 6$, namely $x_0 = 2$, we conclude the entire set of solutions is given by $2 + \mathrm{Ann}(3) = \{2 + b | b \in \mathrm{Ann}(3)\} = \{2, 6, 10\}$, as claimed originally.

---

[1] I.e., degree one. Why is this terminology used

[2] There's a lot that can be said here, but for now we'll concentrate on finding all the other solutions given one.

[3] One could argue that this property follows, for $\mathbb{Z}$ at least, from the fact that multiplication by positive integers respects the additive ordering $<$. We're dancing around the fact that $\mathbb{Z}/n$ can *never* be given an ordering; can you prove this?

[4] Here, $n \in \mathbb{N}$ and $a \in \mathbb{Z}/n$, but we are secretly thinking of a as being an integer between 0 and $n-1$. You should think about what would happen if we replaced a with $a + n$, which represents the same element of $\mathbb{Z}/n$ but has a different factorization.

[5] The ℓ is short for ℓogarithm.

[6] Why do we not want to consider negative numbers here? What is the annihilator of 8 in $\mathbb{Z}/10$?

Exercise. Pick $n \in \mathbb{N}_{>0}$ and $a \in \mathbb{Z}/n$, $a \neq 0$.

(a) Show that $\mathrm{Ann}(a)$ is always the set of multiples of a single element $d \in \mathbb{Z}/n$.

(b) Show that the number d from part (a) is given by $n/(n, a)$.

(c) Show that all of this is well-defined: Even though $a = a + n$ in $\mathbb{Z}/n$, it does not matter whether we compute $\mathrm{Ann}(a)$ or $\mathrm{Ann}(a + n)$ using the technique of parts (a) and (b). More generally, we get the same result for $\mathrm{Ann}(a + bn)$ for all $b \in \mathbb{Z}$.

If we accept the previous Exercise as proved, what can we say about the annihilator of a in $\mathbb{Z}/n$ when a and n are relatively prime, or $(n, a) = 1$? Every element of $\mathrm{Ann}(a)$ is then a multiple of $n/(n, a) = n$, but $n = 0$ in $\mathbb{Z}/n$. Therefore, if $ab = 1$ and $(a, n) = 1$, we conclude that $b = 0$. That is, a is *not* a zero divisor.

As an exercise at the end of the last problem set, you were asked to show that if a is a zero divisor, then a is not invertible and if a is invertible then a is not a zero divisor. Note that this does not say that any element must be either invertible or a zero divisor (or 0).[7] However, in $\mathbb{Z}/n$, this very happy situation does come to pass.

Notation 3. Denote the set of invertible elements of $\mathbb{Z}/n$ by $(\mathbb{Z}/n)^\times$.

Theorem 4. *Pick $n \in \mathbb{N}_{>0}$ and $a \in \mathbb{Z}/n$, $a \neq 0$. Then $a \in (\mathbb{Z}/n)^\times$ if and only if $(a, n) = 1$. If $(a, n) \neq 1$, then a is a zero divisor.*

Proof. If a is invertible[8] then there is some $b \in \mathbb{Z}/n$ such that $ab = 1$. Viewed as integers, this means that $ab \mod n = 1$, or there is some $q \in \mathbb{Z}$ such that $ab = qn + 1$. We can therefore write $1 = ab - qn$, showing[9] that $1 = (a, n)$. The opposite implication is obtained by reading the previous sentence backwards.

If $(a, n) \neq 1$, then $b := n/(a, n) \neq 0$ and $ab = 0$. Thus a nonzero element is either invertible or a zero element,[10] as desired. □

We close with a little bit of group theory, without mentioning groups.[11]

Definition 5. Euler's *totient function* φ assigns to each nonzero number n the number $\varphi(n)$ of natural number a such that $1 \leq a \leq n$ and $(a, n) = 1$.

This entire lecture is really saying that $|(\mathbb{Z}/n)^\times| = \varphi(n)$.[12]

Theorem 6. *For $a \in (\mathbb{Z}/n)^\times$, we have $a^{\varphi(n)} := \underbrace{a \cdot a \cdot \ldots \cdot a}_{\varphi(n)} = 1$.*

Proof. Let $(\mathbb{Z}/n)^\times = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$. Then, as the product of units is again a unit[13], we have $ax_i = x_{\sigma(i)}$ for some function $\sigma : \{1, 2, \ldots, \varphi(n)\} \to \{1, 2, \ldots, \varphi(n)\}$. Moreover, if $ax_i = ax_j$, then $x_i = x_j$, so if $\sigma(i) = \sigma(j)$, then $i = j$.[14] Thus σ applied to $\{1, 2, \ldots, \varphi(n)\}$ is simply writing the same numbers in a different order. Thus

$$\prod_{i=1}^{\varphi(n)} x_i = \prod_{i=1}^{\varphi(n)} x_{\sigma(i)} = \prod_{i=1}^{\varphi(n)} ax_i = a^{\varphi(n)} \cdot \prod_{i=1}^{\varphi(n)} x_i,$$

from which it follows that $a^{\varphi(n)} = 1$, as claimed. □

[7] Consider $2 \in \mathbb{Z}$.

[8] Such an element is often called a *unit*, a term that I'll use freely from now on.

[9] Recall our construction of the GCD.

[10] But never both!

[11] Ignore this sentence.

[12] The vertical bars $|\cdot|$ denote the *cardinality*, or size, of the set of units in $\mathbb{Z}/n$.

[13] Cf. your homework.

[14] Such a function is call *injective*; we will study this an related concepts soon.