Modular Arithmetic

CS255

Chris Pollett

Apr. 5, 2006.

Outline

- More Modular Arithmetic

More on Groups Defined by Modular Arithmetic

- We often are lazy and write b for the element $[b]_n$.
- We further write b^{-1} for the inverse of b mod n. For example, $-2 = (5)^{-1}$ mod 11.
- The size of Z_n^* is denoted by $\phi(n)$, called Euler's phi function.
- It satisfies the equation $$\phi(n) = n \prod_{p|n} (1 - 1/p)$$
- If (S, ⊕), then a subset S' of S that is also a group under ⊕, is called a subgroup of S.

Theorem. If (S, ⊕) is a finite group and S' is any nonempty set of S closed under ⊕, then (S', ⊕) is a subgroup of (S', ⊕).

Theorem. (Lagrange) If (S, ⊕) is a finite group and (S', ⊕) is a subgroup, then |S'| is a divisor of |S|.

Subgroups Generated By an Element

- Given a subset X of a group G. Let $\langle X \rangle$ be the closure of X under the group operation.
- Where G is finite $\langle X \rangle$ is a finite group called the group generated by X.
- In the case where $X=\{b\}$ is a single element, then we write $\langle b \rangle$.
- So $\langle b \rangle = \{b^{(k)} : k>=1\}$ where $b^{(k)}$ means $b \oplus b \ldots \oplus b$ (k times).
- For example in Z_6, $\langle 2 \rangle=\{0,2,4\}$; in Z^*_7, $\langle 2 \rangle = \{1, 2, 4\}$.
- The **order** of a in S, denoted by ord(a), is defined as the smallest positive integer t such that $a^{(t)}=e$.

Theorem. For any finite group $(S, \oplus)$ and any $a \in S$, $\mathrm{ord}(a) = |\langle a \rangle|$.

Proof. Let $t=\mathrm{ord}(a)$. Since $a^{(t)} = e$ and $a^{(t+k)}= a^{(t)} \oplus a^{(k)}=a^{(k)}$ for $k \geq 1$, if $i>t$, then $a^{(i)}=a^{(j)}$ for some $j <t$. Thus, no elements are seen after $a^{(t)}$. So $\langle a \rangle =\{a^{(1)}, a^{(2)},\ldots a^{(t)}\}$ and $|\langle a \rangle| \leq t$. To see $|\langle a \rangle| \geq t$, suppose $a^{(i)}=a^{(j)}$ for some i,j, satisfying $1\leq i < j \leq t$. Then, $a^{(i+k)}=a^{(j+k)}$ for $k>=0$. But this implies $a^{(i+(t-j))}=a^{(j+(t-j))}=e$, a contradiction as $i+(t-j) <t$. So all of of $a^{(i)}$ are distinct.

Some Corollaries

Corollary. The sequence $a^{(1)}$, $a^{(2)}$, .. is periodic with period ord(a).

Corollary. If (S, $\oplus$) is a finite group with identity e, then for all a in S, $a^{(|s|)}$=e.

Solving Modular Linear Equations

- We now look at the problem of finding solutions to the equation

  $ax \equiv b \pmod{n}$

  where a>0 and n>0.
- This is used in one of the steps in the RSA algorithm.
- Let's start with Z_n.

Theorem (%%). For any positive integers a and n, if d=gcd(a,n) then <a> = <d> in Z_n. Thus, |<a>| =n/d.

Proof. We begin by showing that d is <a>. Recall that Extended-Euclid(a,n) produces integers x' and y' such that ax'+ny' =d. Thus ax' ≡ d (mod n), so d is in <a>. Since d is in <a> it follows that every multiple of d is in <a>. So <d> is contained in <a>. But now if m∈<a>, then m = ax mod n. So m = ax+ny. Since d | a and d | n, d | m; so m∈<d>. Therefore <a>⊆<d>.

Corollary. The equation ax ≡ b (mod n) is solvable for the unknown x iff gcd(a,n) | b.

More on Solving Linear Equations

Corollary. The equation $ax \equiv b \pmod{n}$ either has d distinct solutions modulo n, where $d = \gcd(a,n)$, or it has not solutions.

Proof. If $ax \equiv b \pmod{n}$ has a solution, then $b \in \langle a \rangle$. As $\mathrm{ord}(a)=|\langle a \rangle|$, by Theorem (%%), the sequence **Seq** $=\{ai \bmod n \mid i= 0, 1,\ldots,\}$ is periodic with period $|\langle a \rangle| = n/d$. So if $b \in \langle a \rangle$, then b appears exactly d times in **Seq.**