1

MATH 407

2/26/18

Example:

$$2^n \pmod 7$$

$$2^0 \equiv 1 \pmod 7$$
$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$2^3 = 8 \equiv 1 \pmod 7$$
$$2^0 \equiv 2^3 \pmod 7$$

$2^k \equiv 2^{k+3} \pmod 7$ (periodic period 3)

Let $f: A \rightarrow A$ be a function w/ domain (A).

If $f^i(x) = f^{i+k}(x)$ then

$f^j(x) = f^{j+k}(x)$ all subsequent j

May show all periods of $f^n(x)$ are multiples of smallest period.

Pf. Let p be smallest period of $f^n(x)$.
Let k be another " " " ".

Then:

$$k = qp + r \text{ w/ } 0 \leq r < p$$

$$f^i(x) = f^{i+k}(x) = f^{i+qp+r}(x)$$
$$= f^{i+r}(x)$$

(*) Linear Congruences:

$$ax \equiv b \pmod{n}$$

$$ax \equiv 0 \pmod{n}$$

General solution:

Let $d = \gcd(a, n)$

$$a' = \frac{a}{d}, \quad n' = \frac{n}{d}$$

$$\gcd(a', n') = 1$$

$$\begin{aligned} ax \equiv 0 \pmod{7} \ &\text{iff } n \mid ax \quad \text{(homogeneous)} \\ &\text{iff } n'd \mid a'dx \\ &\text{iff } n' \mid a'x \\ &\text{iff } n' \mid x \\ &\text{iff } x \in n'\mathbb{Z} \end{aligned}$$

<u>Thm.</u> $ax_1 \equiv b \pmod{n}$ (heterogeneous)
$ax_2 \equiv b \pmod{n}$

Imply $a(x_1 - x_2) \equiv 0 \pmod{n}$

If $ay \equiv 0 \pmod{n}$, $x_2 = x_1 + y$
satisfies $ax_2 = b$ if $ax_1 = b$

$\therefore$ $x_1 + n'\mathbb{Z}$ is the general solution to $ax = b$
if x_1 is particular solution.

(3)

$ax \equiv b \pmod{n}$
$a = a'd,\ n = n'd$
$a'dx \equiv b \pmod{n'd}$

$a'dx - b = q(n'd)$

$a'dx - qn'd = b$
$(a'x - qn')d = b$

Thm. $ax \equiv b \pmod{n}$ has a solution x
iff $d = \gcd(a,n) \mid b$

Pf. Suppose $d \mid b$ so $b'd = b$.

We want
$$(a'd)x \equiv b'd \pmod{n}$$
$$(n'd) \mid (a'd)x - b'd$$

$$\Rightarrow n' \mid a'x - b'$$
$$a'x \equiv b' \pmod{n}$$

$$\gcd(a', n') = 1$$

Thm. $ax \equiv 1 \pmod{n}$ iff $(a,n) = 1$ for some x.

Pf. There are integers x, y

$$ax + ny = 1$$
$$ax - 1 = n(-y) \equiv 0 \pmod{n}$$
$$ax \equiv 1 \pmod{n}$$

* Find x_1, s.t. $a'x_1 \equiv 1 \pmod{n'}$.

Let x_2 be $b'x_1$

$$\begin{aligned} a'(b'x_1) &\equiv \\ (a'x_1)b' &\equiv \\ 1 \cdot b' &\equiv b' \pmod{n'} \end{aligned}$$

* Example: $(83, 38) = 1$

$$\begin{bmatrix} 1 & 0 & \vdots & 83 \\ 0 & 1 & \vdots & 38 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} 11 & -24 & \vdots & 1 \\ -38 & 83 & \vdots & 0 \end{bmatrix}$$

$1 = 11 \cdot 83 - 24 \cdot 38$

$11 \cdot 83 \equiv 1 \pmod{38}$

$-24 \cdot 38 \equiv 1 \pmod{83} \Rightarrow 59 \cdot 38 \equiv 1 \pmod{83}$

Solve: $11x \equiv 12 \pmod{38}$

$11x \equiv 1 \pmod{38}$

If $x = 83$, $11 \cdot (12 \cdot 83) \equiv 12 \pmod{38}$

$x = 12 \cdot 83$ (a particular solution)

$x = 12 \cdot 83 + 38 \cdot \mathbb{Z}$ (general solution)

* HW on Sec. 1.2 due Wednesday *