Solving modular linear equations

7 Subgroups Generated by an Element

set of elements generated by $a \in S$:

For groups $G = (S, \circ)$ and $a \in S$ define

$$a^{(0)} = e, \ , a^{(i+1)} = a \circ a^{(i)}$$

$$\langle a \rangle = \{a^{(i)} : i \in \mathbb{N}_0\}$$

examples

- in $\mathbb{Z}$:
$$\langle 1 \rangle = \mathbb{N}_0$$
- in $\mathbb{Z}_6$:
$$\langle 2 \rangle = \{0, 2, 4, \}$$
- in Z_7:
$$\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6\}$$
- in Z_n
$$\langle a \rangle = \{ax \bmod n \ : \ x \in \mathbb{N}_0\}$$

7 Subgroups Generated by an Element

set of elements generated by $a \in S$:

For groups $G = (S, \circ)$ and $a \in S$ define

$$a^{(0)} = e, \ , a^{(i+1)} = a \circ a^{(i)}$$

$$\langle a \rangle = \{a^{(i)} : i \in \mathbb{N}_0\}$$

examples

- in $\mathbb{Z}$:
$$\langle 1 \rangle = \mathbb{N}_0$$
- in $\mathbb{Z}_6$:
$$\langle 2 \rangle = \{0, 2, 4, \}$$
- in Z_7:
$$\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6\}$$
- in Z_n
$$\langle a \rangle = \{ax \bmod n \ : \ x \in \mathbb{N}_0\}$$

Lemma 14. *If S is finite and $a \in S$, then $\langle a \rangle$ is a subgroup of S*

7 Subgroups Generated by an Element

set of elements generated by $a \in S$:

For groups $G = (S, \circ)$ and $a \in S$ define

$$a^{(0)} = e, \ , a^{(i+1)} = a \circ a^{(i)}$$

$$\langle a \rangle = \{a^{(i)} : i \in \mathbb{N}_0\}$$

examples

- in $\mathbb{Z}$:
$$\langle 1 \rangle = \mathbb{N}_0$$
- in $\mathbb{Z}_6$:
$$\langle 2 \rangle = \{0, 2, 4, \}$$
- in Z_7:
$$\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6\}$$
- in Z_n
$$\langle a \rangle = \{ax \bmod n \ : \ x \in \mathbb{N}_0\}$$

Lemma 14. *If S is finite and $a \in S$, then $\langle a \rangle$ is a subgroup of S*

Proof.

- S finite $\rightarrow \langle a \rangle \subseteq S$ finite:
$$\exists i, k.\ a^{(i)} = a^{(i+k)} \quad \text{(pigeon hole argument)}$$

7 Subgroups Generated by an Element

set of elements generated by $a \in S$:

For groups $G = (S, \circ)$ and $a \in S$ define

$$a^{(0)} = e, \ , a^{(i+1)} = a \circ a^{(i)}$$

$$\langle a \rangle = \{a^{(i)} : i \in \mathbb{N}_0\}$$

examples

- in $\mathbb{Z}$:
$$\langle 1 \rangle = \mathbb{N}_0$$
- in $\mathbb{Z}_6$:
$$\langle 2 \rangle = \{0, 2, 4, \}$$
- in Z_7:
$$\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6\}$$
- in Z_n
$$\langle a \rangle = \{ax \bmod n \ : \ x \in \mathbb{N}_0\}$$

Lemma 14. *If S is finite and $a \in S$, then $\langle a \rangle$ is a subgroup of S*

Proof.

- S finite $\rightarrow \langle a \rangle \subseteq S$ finite:
$$\exists i, k. \ a^{(i)} = a^{(i+k)} \quad \text{(pigeon hole argument)}$$
- let $h \in S$ be inverse of $a^{(i)}$. Then
$$\begin{aligned} e &= h \circ a^{(i)} \\ &= h \circ a^{(i+k)} \\ &= h \circ a^{(i)} \circ a^{(k)} \quad \text{(associativity)} \\ &= a^{(k)} \end{aligned}$$
- inverse of $a^{(x)}$:
$$\begin{aligned} a^{(x)} \circ a^{(x(k-1))} &= a^{(xk)} \\ &= \circ_{i=1}^{x} a^{(k)} \quad \text{(associativity)} \\ &= \circ_{i=1}^{x} e \\ &= e \end{aligned}$$
- uniqueness: inverses are already unique in S.

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \ : \ a^{(t)} = e\}$$

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \,:\, a^{(t)} = e\}$$

Lemma 15. *If $(s, \circ)$ is a finite group and $a \in S$ then*

$$t = ord(a) = |\langle a \rangle|$$

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \ : \ a^{(t)} = e\}$$

Lemma 15. *If $(s, \circ)$ is a finite group and $a \in S$ then*

$$t = ord(a) = |\langle a \rangle|$$

- $|\langle a \rangle| \leq t$:

$$\{a^{(1)}, \ldots, a^{(t)}\} \subseteq \langle a \rangle$$

For $i > t$ we have

$$\begin{aligned} i &= qt + j \quad \text{with } j < t \\ a^{(i)} &= a^{tq} \circ a^{(j)} \quad \text{(associativity)} \\ &= e \circ a^{(j)} \\ \langle a \rangle &\subseteq \{a^{(1)}, \ldots, a^{(t)}\} \end{aligned}$$

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \ : \ a^{(t)} = e\}$$

Lemma 15. *If $(s, \circ)$ is a finite group and $a \in S$ then*

$$t = ord(a) = |\langle a \rangle|$$

- $|\langle a \rangle| \leq t$:

$$\{a^{(1)}, \ldots, a^{(t)}\} \subseteq \langle a \rangle$$

For $i > t$ we have

$$\begin{aligned} i &= qt + j \quad \text{with } j < t \\ a^{(i)} &= a^{tq} \circ a^{(j)} \quad \text{(associativity)} \\ &= e \circ a^{(j)} \\ \langle a \rangle &\subseteq \{a^{(1)}, \ldots, a^{(t)}\} \end{aligned}$$

- $|\langle a \rangle| \geq t$:

assume

$$a^{(i)} = a^{(j)} \quad \text{with } 1 \leq i < j \leq t$$

then

$$\begin{aligned} a^{(i+k)} &= a^{(j+k)} \quad \text{for all } k \geq 0 \\ a^{(i+(t-j))} &= a^{(j+(t-j))} \\ &= e \\ i + (t-j) &< t \end{aligned}$$

contradicting minimality of t.

$$|\langle a \rangle| \geq |\{a^{(1)}, \ldots, a^{(t)}\}| = t$$

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \ : \ a^{(t)} = e\}$$

Lemma 15. *If $(s, \circ)$ is a finite group and $a \in S$ then*

$$t = ord(a) = |\langle a \rangle|$$

- $|\langle a \rangle| \leq t$:

$$\{a^{(1)}, \dots, a^{(t)}\} \subseteq \langle a \rangle$$

For $i > t$ we have

$$\begin{array}{rcll} i & = & qt + j & \text{with } j < t \\ a^{(i)} & = & a^{tq} \circ a^{(j)} & \text{(associativity)} \\ & = & e \circ a^{(j)} & \\ \langle a \rangle & \subseteq & \{a^{(1)}, \dots, a^{(t)}\} & \end{array}$$

- $|\langle a \rangle| \geq t$:

assume

$$a^{(i)} = a^{(j)} \quad \text{with } 1 \leq i < j \leq t$$

then

$$\begin{array}{rcll} a^{(i+k)} & = & a^{(j+k)} & \text{for all } k \geq 0 \\ a^{(i+(t-j))} & = & a^{(j+(t-j))} & \\ & = & e & \\ i + (t-j) & < & t & \end{array}$$

contradicting minimality of t.

$$|\langle a \rangle| \geq |\{a^{(1)}, \dots, a^{(t)}\}| = t$$

Lemma 16. *Sequence $a^{(0)}, a^{(1)}, \dots$ is periodic with period t, i.e. for all i, j:*

$$i \equiv j \bmod t \ \leftrightarrow \ a^{(i)} = a^{(j)}$$

7 Subgroups Generated by an Element

order of element a in finite group:

$$ord(a) = \min\{t > 0 \ : \ a^{(t)} = e\}$$

Lemma 15. *If $(s, \circ)$ is a finite group and $a \in S$ then*

$$t = ord(a) = |\langle a \rangle|$$

- $|\langle a \rangle| \leq t$:

$$\{a^{(1)}, \dots, a^{(t)}\} \subseteq \langle a \rangle$$

For $i > t$ we have

$$\begin{array}{rcl} i &=& qt + j \quad \text{with } j < t \\ a^{(i)} &=& a^{tq} \circ a^{(j)} \quad \text{(associativity)} \\ &=& e \circ a^{(j)} \\ \langle a \rangle &\subseteq& \{a^{(1)}, \dots, a^{(t)}\} \end{array}$$

- $|\langle a \rangle| \geq t$:

assume

$$a^{(i)} = a^{(j)} \quad \text{with } 1 \leq i < j \leq t$$

then

$$\begin{array}{rcl} a^{(i+k)} &=& a^{(j+k)} \quad \text{for all } k \geq 0 \\ a^{(i+(t-j))} &=& a^{(j+(t-j))} \\ &=& e \\ i + (t-j) &<& t \end{array}$$

contradicting minimality of t.

$$|\langle a \rangle| \geq |\{a^{(1)}, \dots, a^{(t)}\}| = t$$

Lemma 16. *Sequence $a^{(0)}, a^{(1)}, \dots$ is periodic with period t, i.e. for all i, j:*

$$i \equiv j \bmod t \ \leftrightarrow \ a^{(i)} = a^{(j)}$$

Lemma 17. *If $(S, \circ)$ is a finite group with identity e, then*

$$a^{(|S|)} = e \quad \textit{for all } a \in S$$

Let $t = ord(a) = |\langle a \rangle|$, then by Lagrange's theorem (lemma 12)

$$t \mid |S| \quad , \quad |S| \equiv 0 \bmod t$$
$$a^{(|S|)} = a^{(0)} = e$$

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

Lemma 18. *For* $a, n \in \mathbb{N}$ *let* $d = gcd(a, n)$*. Then in* $\mathbb{Z}_n$*:*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d) - 1)d\}$$

Hence

$$|\langle a \rangle| = n/d$$

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

Lemma 18. *For $a, n \in \mathbb{N}$ let $d = gcd(a,n)$. Then in $\mathbb{Z}_n$:*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d)-1)d\}$$

Hence

$$|\langle a \rangle| = n/d$$

- $\langle d \rangle \subseteq \langle a \rangle$: let

  $$(d, x', y') = ext - eucl(a,n)$$

  then

  $$\begin{array}{rcl} d & = & ax' + ny' \\ ax' & \equiv & d \bmod n \\ d & \in & \langle a \rangle \\ \{0, d, 2d, \ldots, ((n/d)-1)d\} & \subseteq & \langle a \rangle \end{array}$$

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

Lemma 18. *For $a,n \in \mathbb{N}$ let $d = gcd(a,n)$. Then in $\mathbb{Z}_n$:*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d)-1)d\}$$

Hence

$$|\langle a \rangle| = n/d$$

- $\langle d \rangle \subseteq \langle a \rangle$: let

  $$(d, x', y') = ext - eucl(a,n)$$

  then

  $$\begin{aligned} d &= ax' + ny' \\ ax' &\equiv d \bmod n \\ d &\in \langle a \rangle \\ \{0, d, 2d, \ldots, ((n/d)-1)d\} &\subseteq \langle a \rangle \end{aligned}$$

- $\langle a \rangle \subseteq \langle d \rangle$: let $m \in \langle a \rangle$. Then

  $$\begin{aligned} m &= ax \bmod n \quad \text{with } x \in \mathbb{Z} \\ m &= ax + ny \quad \text{with } y \in \mathbb{Z} \end{aligned}$$

  $$d|a\ , d|n \quad \rightarrow \quad d|m \quad ; \quad m \in \langle d \rangle$$

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

Lemma 18. *For $a,n \in \mathbb{N}$ let $d = gcd(a,n)$. Then in $\mathbb{Z}_n$:*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d)-1)d\}$$

Hence

$$|\langle a \rangle| = n/d$$

- $\langle d \rangle \subseteq \langle a \rangle$: let

  $$(d, x', y') = ext - eucl(a,n)$$

  then

  $$\begin{aligned} d &= ax' + ny' \\ ax' &\equiv d \bmod n \\ d &\in \langle a \rangle \\ \{0, d, 2d, \ldots, ((n/d)-1)d\} &\subseteq \langle a \rangle \end{aligned}$$

- $\langle a \rangle \subseteq \langle d \rangle$: let $m \in \langle a \rangle$. Then

  $$\begin{aligned} m &= ax \bmod n \quad \text{with } x \in \mathbb{Z} \\ m &= ax + ny \quad \text{with } y \in \mathbb{Z} \end{aligned}$$

  $$d|a\ , d|n \quad \rightarrow \quad d|m \quad ; \quad m \in \langle d \rangle$$

Lemma 19. *Let $d = gcd(a,n)$. Then*

$$ax \equiv b \bmod n$$

is solvalble if and only if $d|b$.

8 Solving modular linear equations

goal:

$$\text{solve} \quad ax \equiv b \bmod n$$

Lemma 18. *For $a, n \in \mathbb{N}$ let $d = gcd(a,n)$. Then in $\mathbb{Z}_n$:*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d)-1)d\}$$

Hence

$$|\langle a \rangle| = n/d$$

- $\langle d \rangle \subseteq \langle a \rangle$: let

  $$(d, x', y') = ext - eucl(a,n)$$

  then

  $$\begin{aligned} d &= ax' + ny' \\ ax' &\equiv d \bmod n \\ d &\in \langle a \rangle \\ \{0, d, 2d, \ldots, ((n/d)-1)d\} &\subseteq \langle a \rangle \end{aligned}$$

- $\langle a \rangle \subseteq \langle d \rangle$: let $m \in \langle a \rangle$. Then

  $$\begin{aligned} m &= ax \bmod n \quad \text{with } x \in \mathbb{Z} \\ m &= ax + ny \quad \text{with } y \in \mathbb{Z} \end{aligned}$$

  $$d|a, d|n \quad \rightarrow \quad d|m \quad ; \quad m \in \langle d \rangle$$

Lemma 19. *Let $d = gcd(a,n)$. Then*

$$ax \equiv b \bmod n$$

is solvalble if and only if $d|b$.

$$\begin{aligned} ax &\equiv b \bmod n \quad \text{solvable} \\ \leftrightarrow b \bmod n &\in \langle a \rangle \\ \leftrightarrow b \bmod n &\in \{0, d, 2d, \ldots, ((n/d)-1)d\} \quad \text{(lemma 18)} \\ \leftrightarrow d &\mid b \bmod n \end{aligned}$$

$$\begin{aligned} b \bmod n &= b + yn \quad \text{with } y \in \mathbb{Z} \\ &= b + yzd \quad \text{with } z \in \mathbb{Z} \quad (d|n) \\ d|b \bmod n &\leftrightarrow d|b \end{aligned}$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \; : \; ax \equiv b \bmod n\}| \in \{0, d\}$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \ : \ ax \equiv b \bmod n\}| \in \{0, d\}$$

- If $ax \equiv b \bmod n$ is solvable, then

$$\begin{aligned} b \bmod n &\in \langle a \rangle \\ \leftrightarrow b \bmod n &\in \{0,,d,2d,\dots((n/d)-1)d\} \quad \text{(lemma 18)} \end{aligned}$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \;:\; ax \equiv b \bmod n\}| \in \{0, d\}$$

- If $ax \equiv b \bmod n$ is solvable, then

$$\begin{aligned} b \bmod n &\in \langle a \rangle \\ \leftrightarrow b \bmod n &\in \{0,,d,2d,\ldots((n/d)-1)d\} \quad \text{(lemma 18)} \end{aligned}$$

- lemmas 16 and 18 $\rightarrow$

sequence $s = (\, a^{(0)}, a^{(1)}, \ldots, a^{(n-1)})$ periodic with period $|\langle a \rangle| = n/d$

$$a^{(x)} = ax \bmod n \quad \text{for candidate solutions } \; x = 0,1,\ldots n-1 \in \mathbb{Z}_n$$

$$s = (a^{(0)},\ldots a^{(n/d-1)} \ldots a^{(0)},\ldots a^{(n/d-1)}) \text{ repeated } d \text{ times}$$

As

$$b \bmod n \in \langle a \rangle = \{a^{(0)},\ldots a^{(n/d-1)}\}$$

each of the d blocks contains exactly one x solving $a^{(x)} = b \bmod n$.

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \,:\, ax \equiv b \bmod n\}| \in \{0, d\}$$

- If $ax \equiv b \bmod n$ is solvable, then

$$\begin{aligned} b \bmod n &\in \langle a \rangle \\ \leftrightarrow b \bmod n &\in \{0,,d,2d,\ldots((n/d)-1)d\} \quad \text{(lemma 18)} \end{aligned}$$

- lemmas 16 and 18 $\rightarrow$

sequence $s = (\, a^{(0)}, a^{(1)}, \ldots, a^{(n-1)})$ periodic with period $|\langle a \rangle| = n/d$

$$a^{(x)} = ax \bmod n \quad \text{for candidate solutions } \; x = 0, 1, \ldots n-1 \in \mathbb{Z}_n$$
$$s = (a^{(0)}, \ldots a^{(n/d-1)} \ldots a^{(0)}, \ldots a^{(n/d-1)}) \text{ repeated } d \text{ times}$$

As

$$b \bmod n \in \langle a \rangle = \{a^{(0)}, \ldots a^{(n/d-1)}\}$$

each of the d blocks contains exactly one x solving $a^{(x)} = b \bmod n$.

one solution:

Lemma 21. *Let*

$$d = gcd(a,n)\ ,\ d = ax' + ny'\ ,\ d|b$$

Then

$$x_0 = x'(b/d) \bmod n \quad \textit{solves} \quad ax \equiv b \quad \bmod n$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \ : \ ax \equiv b \bmod n\}| \in \{0, d\}$$

- If $ax \equiv b \bmod n$ is solvable, then

$$\begin{aligned} b \bmod n &\in \langle a \rangle \\ \leftrightarrow b \bmod n &\in \{0,,d,2d,\ldots((n/d)-1)d\} \quad \text{(lemma 18)} \end{aligned}$$

- lemmas 16 and 18 $\rightarrow$

sequence $s = (\ a^{(0)}, a^{(1)}, \ldots, a^{(n-1)})$ periodic with period $|\langle a \rangle| = n/d$

$$a^{(x)} = ax \bmod n \quad \text{for candidate solutions } \ x = 0,1,\ldots n-1 \in \mathbb{Z}_n$$

$$s = (a^{(0)}, \ldots a^{(n/d-1)} \ldots a^{(0)}, \ldots a^{(n/d-1)}) \text{ repeated } d \text{ times}$$

As

$$b \bmod n \in \langle a \rangle = \{a^{(0)}, \ldots a^{(n/d-1)}\}$$

each of the d blocks contains exactly one x solving $a^{(x)} = b \bmod n$.

one solution:

Lemma 21. *Let*

$$d = gcd(a,n) \ , \ d = ax' + ny' \ , \ d|b$$

Then

$$x_0 = x'(b/d) \bmod n \quad \textit{solves} \quad ax \equiv b \quad \bmod n$$

$$\begin{aligned} ax_0 &\equiv ax'(b/d) \bmod n \\ &\equiv d(b/d) \bmod n \quad (ax' \equiv d \bmod n) \\ &\equiv b \bmod n \end{aligned}$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \ : \ ax \equiv b \bmod n\}| \in \{0, d\}$$

one solution:

Lemma 21. *Let*

$$d = gcd(a,n) \ , \ d = ax' + ny' \ , \ d|b$$

Then

$$x_0 = x'(b/d) \bmod n \quad solves \quad ax \equiv b \mod n$$

d **solutions:**

Lemma 22. *Let*

$$d = gcd(a,n) \ , \ d|b \ , \ x_0 \quad solves \quad ax \equiv b \mod n$$

Then the d distinct dolutions of $\quad ax \equiv b \mod n$ *are*

$$x_i = x_0 + i(n/d) \ for \ i \in [0 : d-1]$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \ : \ ax \equiv b \bmod n\}| \in \{0,d\}$$

one solution:

Lemma 21. *Let*

$$d = gcd(a,n)\ ,\ d = ax' + ny'\ ,\ d|b$$

Then

$$x_0 = x'(b/d) \bmod n \quad \textit{solves} \quad ax \equiv b \mod n$$

d solutions:

Lemma 22. *Let*

$$d = gcd(a,n)\ ,\ d|b\ ,\ x_0 \quad \textit{solves} \quad ax \equiv b \mod n$$

Then the d distinct dolutions of $\quad ax \equiv b \mod n$ *are*

$$x_i = x_0 + i(n/d) \textit{ for } i \in [0 : d-1]$$

- distincness

$$\forall i, j \in [0 : d-1]$$

$$i \neq j \quad \rightarrow \quad x_0 + i(n/d) \bmod n \neq x_0 + j(n/d) \bmod n$$

8 Solving modular linear equations

Lemma 20. *Let $d = gcd(a,n)$ then for the number of solutions in $\mathbb{Z}_n$ holds*

$$|\{x \in \mathbb{Z}_n \; : \; ax \equiv b \bmod n\}| \in \{0, d\}$$

one solution:

Lemma 21. *Let*

$$d = gcd(a,n) \;,\; d = ax' + ny' \;,\; d|b$$

Then

$$x_0 = x'(b/d) \bmod n \quad \textit{solves} \quad ax \equiv b \quad \bmod n$$

d **solutions:**

Lemma 22. *Let*

$$d = gcd(a,n) \;,\; d|b \;,\; x_0 \quad \textit{solves} \quad ax \equiv b \quad \bmod n$$

Then the d distinct dolutions of $\quad ax \equiv b \quad \bmod n$ *are*

$$x_i = x_0 + i(n/d) \textit{ for } i \in [0 : d-1]$$

- distincness

$$\forall i, j \in [0 : d-1]$$

$$i \neq j \quad \to \quad x_0 + i(n/d) \bmod n \neq x_0 + j(n/d) \bmod n$$

- solutions

$$\begin{aligned} ax_i \bmod n &= a(x_0 + i(n/d)) \bmod n \\ &= (ax_0 + ain/d) \bmod n \\ &= ax_0 \bmod n \quad (d|a) \\ &\equiv b \bmod n \end{aligned}$$

8 Solving modular linear equations

modular linear equation solver:

$modular - linear - equation - solver(a,b,n)$:

$(d,x',y') = ext - eucl(a,n);$

if $d|b$
{
$x_0 = x'(b/d) \bmod n;$

for $i = 0$ to $d-1$
}
print $(x_0 + i(n/d) \bmod n)$
{
else { print 'no solutions' }

example:

$$14x \equiv 30 \bmod 100 \quad a = 14\ ,\ b = 30\ ,\ n = 100$$

$$ext - eucl(14,100) = (2,-7,1)$$

$$d = 2 = 14(-7) + 1 \cdot 100$$

$$b/d = 30/2 = 15$$

$$x_0 = (-7)(15) \bmod 100 = 95$$

$$x_1 = 95 + (100/2) \bmod 100 = 45$$

8 Solving modular linear equations

modular linear equation solver:

$modular-linear-equation-solver(a,b,n)$:

$(d,x',y') = ext-eucl(a,n);$

if $d|b$
{
$x_0 = x'(b/d) \text{ mod } n;$

for $i = 0$ to $d-1$
}
print $(x_0 + i(n/d) \text{ mod } n)$
{
else { print 'no solutions' }

example:

$$14x \equiv 30 \text{ mod } 100 \quad a = 14\ ,\ b = 30\ ,\ n = 100$$

$$ext-eucl(14,100) = (2,-7,1)$$

$$d = 2 = 14(-7) + 1 \cdot 100$$

$$b/d = 30/2 = 15$$

$$x_0 = (-7)(15) \text{ mod } 100 = 95$$

$$x_1 = 95 + (100/2) \text{ mod } 100 = 45$$

run time[arithmetic operations]:

- ext-eucl: $= O(\log n)$
- for loop: $O(d) = O(gcd(a,n))$ iterations, each with $O(1)$ operations

8 Solving modular linear equations

Lemma 23. *Let $n > 1$. If $gcd(a,n) = 1$ Then $ax \equiv b \bmod n$ has a uniques solution in $\mathbb{Z}_n$.*

Inverses in Z_n^* are unique; Z_n^* is group.

8 Solving modular linear equations

Lemma 23. *Let* $n > 1$. *If* $gcd(a,n) = 1$ *Then* $ax \equiv b \mod n$ *has a uniques solution in* $\mathbb{Z}_n$.

Inverses in Z_n^* are unique; Z_n^* is group.

multiplicative inverses

If x solves $ax \equiv 1 \mod n$, then x is a *multiplicative inverse* of a.

Lemma 24. *Let* $n > 1$. *If* $gcd(a,n) = 1$, *then* $ax \equiv 1 \mod n$ *has a unique solution in* $\mathbb{Z}_n$

Notation: $x = a^{-1}$.

Efficient computation:

$$ext - eucl(a,1,n) = (1,x,y) \quad , \quad 1 = ax + ny$$

$$ax \equiv 1 \mod n \quad , \quad a^{-1} = x \mod n$$