P2 Review Session

~~Structural induction~~

~~RSA example~~
- ~~why mod n?~~

~~Proof of Euler's theorem.~~

Equiv. classes

Base b rep.

~~Def^n of Bézout Coeffs.~~

Weak vs. Strong ind.

~~Functions are well-defined.~~
~~$f: A/R \to X$~~

Finding $\varphi(m)$
(when $m \neq p \cdot q$)

Finding $\varphi(n)$

Def^n: $\varphi(n)$ is # units in $\mathbb{Z}_n$.

Fact: $[a]_n$ is a unit iff $\gcd(a,n)=1$
i.e. if $a \& n$ have no common factors.

Ex: $\varphi(12)$

$\mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$

$\varphi(12) = 4$

Ex: $\varphi(p)$ ← prime

$\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$

$p-1$ units

$\varphi(p) = p-1$

Ex: $\varphi(p \cdot q)$ ← diff. primes

$\mathbb{Z}_{pq} = \{1, \ldots, p-1, p+1, \ldots, 2p-1, \ldots, pq-1\}$

pq total
$-p$ mults of q
$-q$ mults of p
$+1$ double count.

$(p-1)(q-1)$

RSA Example

Sender: msg

Recipient: $n = pq$, $\varphi(n) = (p-1)(q-1)$, choose a unit $[k]_{\varphi(n)}$, find $[k]^{-1}_{\varphi(n)}$ (using Bézout coeffs)

Sender: raise [msg] to large power; cipher text $C = [msg^k]_n$

$[a^b]^c = [a^{bc}]$

$[a]^{[b]_{\varphi(n)}} := [a^b]$

Recipient: raise C to huge power

$C^{[k]^{-1}} = ([msg]^{[k]})^{[k]^{-1}}$

$= [msg]^{([k][k]^{-1})}$

$= [msg]^{[1]} = [msg]$.

Recipient

$p = 5$, $q = 7$, $m = 35$

$\varphi(n) = (p-1)(q-1) = 24$

$[k]_{\varphi(n)}$ a unit. (i.e. $\gcd(k, \varphi(n)) = 1$)

$k = 7$.

$[k]^{-1}_{24}$? $[7]^{-1}_{24}$

msg = 3

k, n → 7, 35

$[k]^{-1} = [7]^{-1} = [7]$

$c = [3^7]_{35} = [17]$

$[17]^{[7]}$

$\downarrow$

$[3]$

$7 = 4 + 2 + 1$

$[3^7] = [3^4] \cdot [3^2] \cdot [3]$

$[3^2] = [9]$ (mod 35)

$[3^4] = [3^2]^2 = [9][9]$

$= [81]_{35}$

$= [11]_{35}$

$[3^4 \cdot 3^2] = [9 \cdot 11] = [99] = [29]_{35}$

$[3^7] = [3^6 \cdot 3] = [27][3] = [87] = [17]$

$C^{[k]^{-1}}$

Bezout Coeffs.

Claim: $\forall a, b, \exists s, t$ with $g(a,b) = sa + tb$. s, t called Bezout Coeffs.

Proof:

$g(a,b) = g(b,r)$ where $a = qb + r$.

Euclid's GCD for g' and t' by induction

inductive step: WTS $\exists s, t$ $g(a,b) = sa + tb$

know $g(a,b) = g(b,r) = s'b + t'r$

$= s'b + t'(a - qb)$

$= t'a + (s' - t'q)b$.

$= sa + tb$.

let $s = t'$

$t = s' - t'q$.

$\gcd(k, \varphi(n)) = s \cdot k + t \cdot \varphi(n)$

$\gcd(7, 24) = 1 = s \cdot 7 + t \cdot 24$

$[1] = [s][k] + [t][\varphi(n)]$ (mod $\varphi(n)$)

$[1] = [s][k]$

$[k]^{-1}_{\varphi(n)}$ is $[s]$.

$g(24,7)$	$a = 7$	$b = 24$	$q = 0$	$r = 7$	$s = 7$	$t = -2$	$1 = 7 \cdot 7 + -2 \cdot 24 = 49 - 48 = 1$ ✓
							$= sa + tb$.
$g(24,7)$	$a' = 24$	$b' = 7$	$q' = 3$	$r = 3$	$s' = -2$	$t' = s'' - t''q'$	$1 = s'a + t'b'$ ✓
						$= 1 + 2 \cdot 3 \cdot 7$	
$g(7,3)$	$a'' = 7$	$b'' = 3$	$q'' = 2$	$r'' = 1$	$s'' = 1$	$t'' = -2$	$1 = s''a'' + t''b''$

⋮

Let $f: A/R \to X$ be given by

$f([a]) := \underbrace{a^2}_{\text{expression using } a.}$

if $[a]=[b]$ then $f([a])$ better be $= f([b])$

$a^2 = b^2$

Ex: let $f: \mathbb{Z}_5 \to \mathbb{Z}$ be given by

$f([a]_5) := a^2$

f is not well defined

$\left(\begin{smallmatrix}\text{mod}\\5\end{smallmatrix}\right)$ $[2]=[7]$ but $2^2 = 4 \neq 7^2 = 49.$

$[2] \xrightarrow{F} 4$

$[2] \xrightarrow{} 49$

$g([a]) := [a^2]$ is well defined

$g[[2]) = [4]$

$g([7]) = [49]$

WTS if $[a]=[b]$ then $[a^2]=[b^2]$

Euler's thm: if $[a]_m$ is a unit, then

(exponentiation is well-defined, if working mod m in a base, mod $\varphi(m)$ in exp.)

$[a]_m^{[b]_{\varphi(m)}} := [a^b]_m$ is well defined.

i.e. if $[a]_m = [a']_m$ and if $[b]_{\varphi(m)} = [b']_{\varphi(m)}$

then $[a^b]_m = [a'^{b'}]_m$.

Proof sketch:

easy: $[a^b] = [a'^b]$

$\underbrace{[a]\cdot[a]\cdots[a]}_{b \text{ times}} = \underbrace{[a']\cdot[a']\cdots[a']}_{b \text{ times}}$

hard: $[a^b] = [a^{b'}]$

using: $[a]^{\varphi(n)} = [1]$ (Euler's theorem v2)

Assume $[b]_{\varphi(n)} = [b']_{\varphi(n)}$, WTS $[a^b] = [a^{b'}]$.

Since $[b]_{\varphi(n)} = [b']_{\varphi(n)}$, $b = b' + c\varphi(n)$ for some c.

Then $[a^b] = [a^{b'+c\varphi(n)}]$

$= [a^{b'} \cdot a^{c\varphi(n)}]$

$= [a^{b'}][[a]^{\varphi(n)}]^c$ (Euler's v2)

$= [a^{b'}][1] = [a^{b'}]$

$[a^{b'}][a^{c\varphi(n)}]$

$[(a^{\varphi(n)})^c]$

$\varphi(10) = 4$

$[3]_{10}^{[2]_4} = [3^2]_{10}$

$\|$ $\updownarrow$

$[3]_{10}^{[6]_4} = [3^6]_{10}$

Sidebar:

Equivalent:

- $[b]_m = [b']_m$
- $b \equiv_m b'$ ~~($b \equiv b'$ (mod m))~~
- $m \mid b - b'$
- $\exists c$ such that $b - b' = mc$
- $b = b' + mc$ for some $c \in \mathbb{Z}$
- $\text{rem}(b, m) = \text{rem}(b', m)$

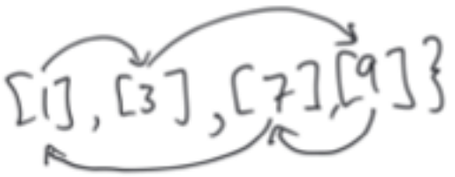
Euler's version 2:

Draw $\mathbb{Z}_n^*$, what happens when multiply by $[a]$

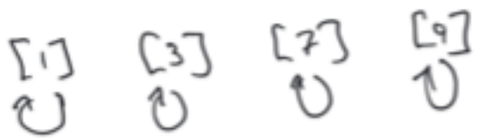
$n=10$

$[a]=[3]$

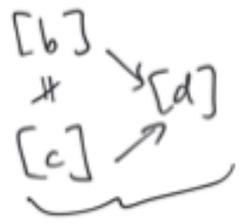
$\mathbb{Z}_{10}^* = \{[1],[3],[7],[9]\}$



$[a]=[1]$



$\xrightarrow{\times[a]}$



can't happen

because this means

$[a][b]=[d]$ and

$[a][c]=[d]$ so

$[b]=[c]$ because $[a]$ is a unit,

so if $[a][b]=[a][c]$

then $[a]^{-1}[a][b] = [a]^{-1}[a][c]$

so $[b]=[c]$.

Structural induction

Inductively defined set

$\varepsilon, \varepsilon a, \varepsilon aa, \varepsilon aaa, \ldots$

$x \in \Sigma^* ::= \varepsilon \mid xa \qquad a \in \Sigma$

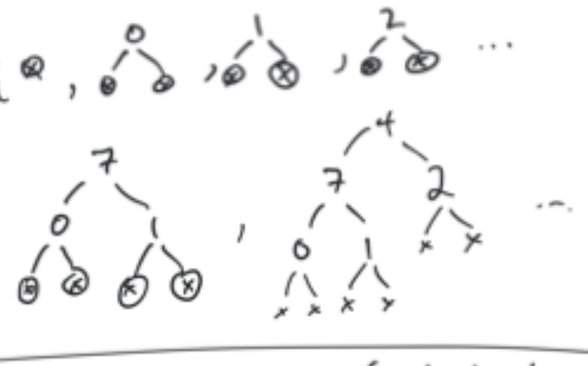
(x: some "smaller" string)

$\Sigma^* = \{\varepsilon, \varepsilon 0, \varepsilon 1, \varepsilon 00, \varepsilon 01, \ldots\} \qquad \Sigma = \{0,1\}$

$\varepsilon 0$ is a substructure of $\varepsilon 00$

$t \in T ::= \otimes \mid \overset{a}{(t_1\ t_2)} \qquad a \in \mathbb{N}$

$T = \{\otimes, \overset{0}{(\otimes\ \otimes)}, \overset{1}{(\otimes\ (\otimes\ \otimes))}, \overset{2}{((\otimes\ \otimes)\ (\otimes\ \otimes))}, \ldots\}$



$n \in \mathbb{N} ::= Z \mid Sn$

$\forall n \in \mathbb{N}, P(n)$

① $P(Z)$ ② $P(Sn)$ assuming $P(n)$ (for arb. n)

② $\forall n$, if $P(n)$ then $P(Sn)$

Proof by struct. ind.

to prove $\forall x \in X, P(x)$

we can prove $P(x)$ for each rule, assuming P(each substructure)

(inductively defined set X)

$x \in \Sigma^* ::= \varepsilon \mid xa \qquad a \in \Sigma$

to prove: $\forall x \in \Sigma^*, \overbrace{len(x) \geq 0}^{P(x)}$

need to show

① $P(\varepsilon)$ ② $P(xa)$ assuming $P(x)$

① $len(\varepsilon) \geq 0$ ② $len(xa) \geq 0$, assuming $len(x) \geq 0$.

$P(x) =$ "$len(x) \geq 0$"

$P(n) =$ "$len(n) \geq 0$"

$P(n') =$ "$len(n') \geq 0$"

---

to prove: $\forall t \in T, P(t)$

$t \in T ::= \otimes \mid \overset{a}{(t_1\ t_2)}$

Show: ① $P(\otimes)$ and

② $P(\overset{a}{(t_1\ t_2)})$ assuming $P(t_1)$ and $P(t_2)$

Inductively defined fn:

to define $f : X \to Y$

$\Uparrow$ inductively defined set.

define $f(x)$ for each rule defining X.

$x \in \Sigma^* ::= \varepsilon \mid xa$ $\quad a \in \Sigma$

Σ^*: set of strings. $\quad \Sigma$: set of characters

$f : \Sigma^* \to \mathbb{N}$

$f(\varepsilon) :=$

$f(xa) :=$ (use $f(x)$, since x is a substructure of xa)

$len(\varepsilon) := 0$

$len(xa) := 1 + len(x)$