Review sess: 2: number theory

2. Computing Bezout coeffs (gcd)
   \#17: finding inverses

RSA
\#2

Fast exp on

Well-defined for $n$

Base $b$

Uniqueness
Q.21: Give a reg. expr. that matches strings of 0s & 1s that, when interpr. in binary are not div. by 3.

HW: Give a DFA accepts strings that are multis of 3 (in binary).

Int: states are \( \mathbb{Z}_3 \).

\( (110)_2 \):

[Diagram showing transitions between states with labels: 0, 1, 2, and the final state labeled 0.]
Claim: \( \forall n, \exists \text{ a base } b \text{ rep of } n \).

Pf: strong ind on \( n \).

WRs P(0), i.e. 0 has a base b rep

WTS P(n), i.e. \( n \) has a base b rep

\[
\text{Ind: last digit is } \text{rem}(n,b) \\
\text{rest of digits are base-b rep of } \text{quot}(n,b) \\
347 \text{ in base } 5
\]

\[ d_0 = \text{rem}(347,5) = 2 \]

rest of digits are base 5 rep of \( \text{quot}(347,5) = 69 \)

\[ 2342 \rightarrow 347 \]

\[ 234 \rightarrow 69 \text{ in base } 5 \]

\[ d_0' = \text{rem}(69,5) = 4 \]

rest: base 5 rep of \( \text{quot}(69,5) = 13 \)

\[ (234)_{b=5} = 13 \text{ in base } 5 \]

\[ d_0 = \text{rem}(13,5) = 3 \]

rest: base 5 rep of \( \text{quot}(13,5) = 2 \)

\[ d_0 = 2 \]

\[ 2 \text{ in base } 5 = (2)_{b=5} \]

Claim: base-b rep is unique (no leading 0s)

Pf: WTS if \( (d_i \ldots d_0)_{b} = (d_i' \ldots d_0')_{b} \)

then \( \forall i, d_i = d_i' \)

by induction

WTS (if \( (x)_{b} = (y)_{b} \) and \( x, y \) don't start \( \text{with } 0 \), then \( x = y \))

Pf: by induction on \( x \) and \( y \).

\[ P(e, z), P(e, y), P(xa, e) \]

\[ x = y' \]

\[ P(xa, y) \]

\[ b \cdot (x)_{b} + a = b \cdot (y)_{b} + c \]

uniqueness of \( \text{rem } \text{ is} \text{ quot.} \)

\( (x)_{b} \) is \text{ quot.} \)
Fast exp.  

\[ b = \text{large } b \]  

\[ a \]  

\[ a^2 = a \cdot a \]  

\[ a^4 = a^2 \cdot a^2 \]  

\[ a^8 = a^4 \cdot a^4 \]  

\[ a^{16} = a^8 \cdot a^8 \]  

\[ a^{32} = a^{16} \cdot a^{16} \]  

\[ \vdots \]  

\[ 19 = (10011)_2 \]  

\[ a^{19} = a^{16} \cdot a^2 \cdot a \]  

\[ b = \text{sum of powers of 2} \]  

\[ b = (d_j \ldots d_0)_2 \]  

\[ = \sum d_i \cdot 2^i \]  

\[ \text{each } d_i \text{ is 0 or 1}. \]  

\[ [a]^b \]  

\[ [a^2] = [a][a] \]  

\[ [a^4] = [a^2][a^2] \]  

\[ [a^8] = [a^4][a^4] \]  

\[ [a^{16}] = [a^8][a^8] \]  

\[ \text{reduce mod } a \text{ anytime}. \]
Euler's Theorem

\[ \left( a^n \right)^{\varphi(n)} \equiv 1 \pmod{n} \]

is well-defined if \([a]_n\) is a unit.

\[ \text{gcd}(a, n) = 1 \]

and \([a]_n\) is a unit iff. \( \phi(n) \mid \lambda(n) \) or \( n \) is a prime.

\[ \varphi(p) = p-1 \]

\[ \varphi(p^k) = (p-1)p^{k-1} \]

**Theorem:** If \([a]_n\) is a unit, then \([a]_n^{\varphi(n)} \equiv 1 \pmod{n} \)

Use this to show \([a]_p \equiv [a]_p \pmod{p} \) if \( p \) is prime.

\[ [a]_p^{p-1} \equiv [1]_p \]

if \([a]_p \) is a unit.

\[ [a][a]^r = [1][1] = [a] \]

if \([a]_p \) is not a unit, then \([a]_p \equiv [a] \pmod{p} \)

and \([0][3] = [0] = [a] \pmod{p} \).
Bézout's identity
\[ ax + by = \gcd(a, b) \]
where \( \gcd(a, b) \) is the greatest common divisor of \( a \) and \( b \).

Ex. Find Bézout's coefficients of 25, 37

\[
\begin{align*}
25 &= 2 \cdot 37 + (-2) \\
37 &= 1 \cdot 25 + 12 \\
25 &= 2 \cdot 12 + 1 \\
12 &= 12 \cdot 1 + 0
\end{align*}
\]

\[ \boxed{\gcd(25, 37) = 1} \]

To find the coefficients, we work backwards:

\[
\begin{align*}
1 &= 12 - 2 \cdot 6 \\
1 &= 12 - 2 \cdot (25 - 2 \cdot 12) \\
1 &= 5 \cdot 25 - 3 \cdot 37
\end{align*}
\]

So the Bézout's coefficients are \( a = -3 \) and \( b = 5 \).

Therefore, the equation is
\[ -3 \cdot 25 + 5 \cdot 37 = 1 \]
Q2: Suppose Bob computes $[k']^t \mod q(m)$ instead of $k^t \mod q(m)$. What decrypted msg does he see?

Bob thinks $[k']^t \leftrightarrow [k^t]$ where

$$[k] [k']^t = [1] \mod 4(p(m))$$

$$1 = [kk']^t = [kk'] \mod 4(p(m))$$

means $kk' = 1 + t \cdot 4(p(m))$

$[k']^t = [msg]_{m}^t = [msg^{-1}]_{m} \cdot [msg]_{m} = [msg^{-1}]_{m} \cdot [msg]_{m} \cdot [msg^{-1}]_{m}^{-1} \cdot [msg]_{m}^{-1} \cdot [msg]_{m}^{-1}$

Euler's thm:

$[a]_m^{\phi(m)} = [1]$

$[a]_m^{\phi(m)} \cdot [a]_m = [a]_m$