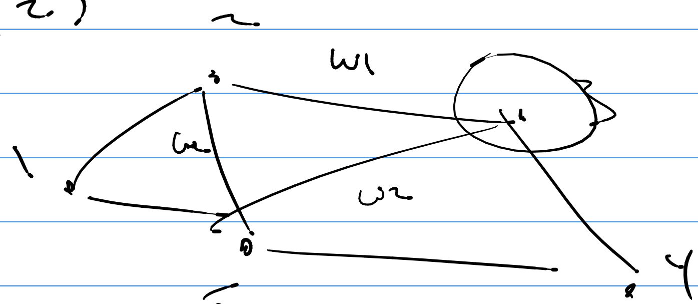
Math 451

Q's / dijk(A, 2)

2	(0)
2-3	(w_1)
&	



2, [3, 4, 1,] 7

is 1 in this? → 1 0 → index v, b+1

no

---

gcd(a,b)

ex. $\gcd(22, 30) = \gcd(2^1 \cdot 11^1, 2^1 \cdot 3^1 \cdot 5^1) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 11^0$

$= 2$

$\text{lcm}(2^1 \cdot 11^1, 2^1 \cdot 3^1 \cdot 5^1) = 2^1 3^1 5^1 11^1$

$= 330$

---

gcd(a,b) ← biggest number that divides a, b

$a = q \cdot b + r \qquad 6 = 3 \cdot 2 + 0$

$30 = 1 \cdot 22 + 8$

→ it divides b, r

$\gcd(a,b) = \gcd(b,r)$

$gcd(30, 22)$
$= gcd(22, 8)$
$= gcd(8, 6)$
$= gcd(6, 2)$
$= 2$

a	= b	+ r
30	= 1·22	+ 8
22	= 2·8	+ 6
8	= 1·6	+ 2
6	= 3·2	+ 0

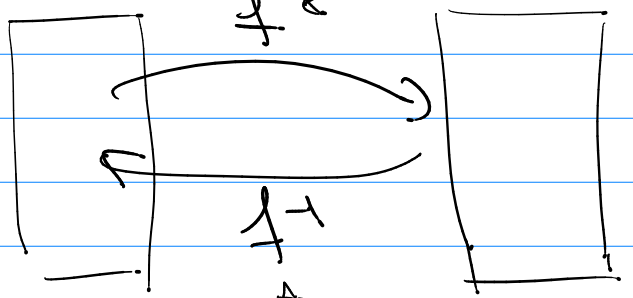
$gcd(a,b) = gcd(b, r)$

Extended GCD $\quad gcd(a,b) = s \cdot a + t \cdot b$

Cryptography

private ⓚ public

invertible function (encryption) f



Private: if f is known, f^{-1} is trivial to find.

Public if f is known, f^{-1} takes a "known" amount of time to find.

Publicity: private key → make public (fix) private

RSA | p, q are primes. ← $p \cdot q = n$ key)

Power of a technique is based on if you are not given f can you still decrypt the message?

block cipher

armKwa serke

1 to 1 replacement

a	b	c	d	e	f	...	z	space
"	"	"	"	"	"		"	
z	g	r	d	m	^		w	~