Number theoretic Algorithms.

$[A]_{m \times n}$ $[B]_{n \times p}$.

Matrix multiplication.

$(a_{11}\ a_{12}\ a_{13}) \begin{pmatrix} b_{p1} \\ b_{21} \\ b_{31} \end{pmatrix}$.

$n \cdot mp$
$= mnp$
$+$

A

$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}_{2 \times 3}$

B.

$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{bmatrix}_{3 \times 2}$

$m = 2$
$n = 3$
$p = 2$

$\begin{bmatrix} c_{11} & - \\ & \\ & \end{bmatrix}_{2 \times 2}$

	Mult	Add
①	3	$2 = 5$
②	3	$2 = 5$
③	3	$2 = 5$
④	3	$2 = 5$.

$T_D(m, n, p) = mnp = 10 \times 20 \times 40$

If this fn $T(\ )$ is a polynomial of its input, then we call the given algorithm as an "efficient" algorithm.

$f(n) = n^3$ vs. $g(n) = 2^n$

$g(50) = 2^{50}$ $\quad f(50) = 50^3$

$g(60) = 2^{60}$ $\quad f(60) = 60^3$

$T_D(n) = n^6 + 5n^2 + 3.$

$T(n) = O(n^6)$

$T'(n) = n^3 + 3n^2$

$T'(n) = O(n^3)$

Euclidean algosithm:-

$a = 15$

$b = 6$

$gcd(15, 6)$

$\Rightarrow gcd(6, 3)$

$6 \overline{)15} \; 2$

12

$3 \overline{)6} \; 2$

6

x

Prop: Let $a, b > 1$ with $b \nmid a$.
Then $\gcd(a, b) = \gcd(b, a \bmod b)$

Pf: If $b > a$, then the claim is obvious.
So, we assume $a > b$.

$a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 < r < b$
Let d be the gcd of a, b. $r = a \bmod b$.
$\Rightarrow d \mid a, d \mid b \Rightarrow d \mid r$.
$d \mid b$, and $d \mid r \Rightarrow d \mid \gcd(b, a \bmod b)$.

Let $d' = gcd(b, a \bmod b)$

$\vdots$

$d' \mid gcd(a, b)$

FACT(n)

↓

FACT(n-1)

↓

FACT(n-2)

↓

FACT(2)

↓

FACT(1) = 1

FACT(5)

↓

5 * FACT(4)

↓

4 * FACT(3)

↓

3 * FACT(2)

↓

2 * FACT(1)

↓

1

Factorial algorithm:

FACT(n) → n!

n * FACT(n-1)

$n! = n * (n-1)!$

Let $d' = gcd(b, a \bmod b)$

$\vdots$

$d' \mid gcd(a, b)$

FACT(n)

↓

FACT(n-1)

↓

FACT(n-2)

↓

FACT(2)

↓

FACT(1) = 1

FACT(5)

↓

5 * FACT(4)

↓

4 * FACT(3)

↓

3 * FACT(2)

↓

2 * FACT(1)

↓

1

Factorial algorithm:

FACT(n) → n!

n * FACT(n-1)

$n! = n * (n-1)!$

Euclidean algorithm:

```
GCD(a, b).                    /* size of a, b represents the length of a, b in terms of no. of bits */
   if b|a then return b       <-- Base condn
   - else return GCD(b, a mod b)
end
```

GCD(27, 12) — 3
  a b
  ↓
GCD(12, 3)

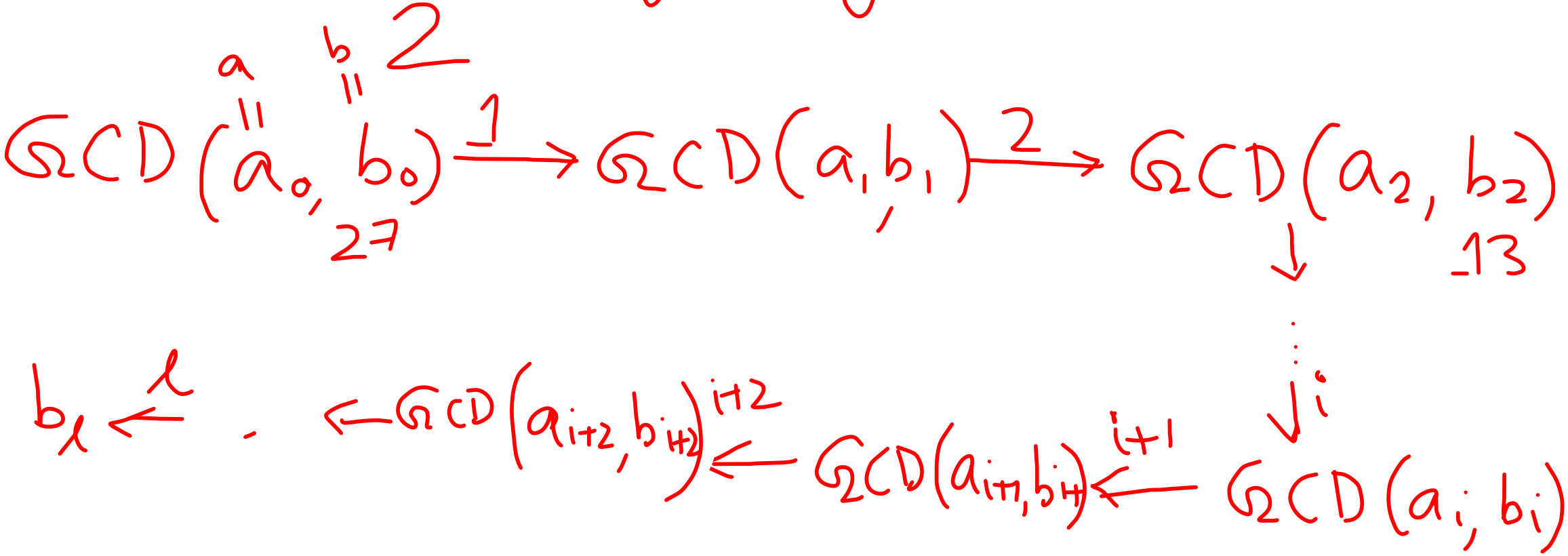
$2\|b\|$

Time complexity = $4\|b\| = O(\|b\|)$

This alg is polynomial time alg.

Prof: Consider an execution of GCD(a_0, b_0) and let a_i, b_i be the arguments to the i^{th} recursive call of GCD. Then

$$b_{i+2} \leq \frac{b_i}{2} \quad \text{for any } 0 \leq i \leq l-2$$



Pf: For any $a > b$, $[a \bmod b] < a/2$.

Suppose $b \le a/2$. $[a \bmod b] < b \le a/2$

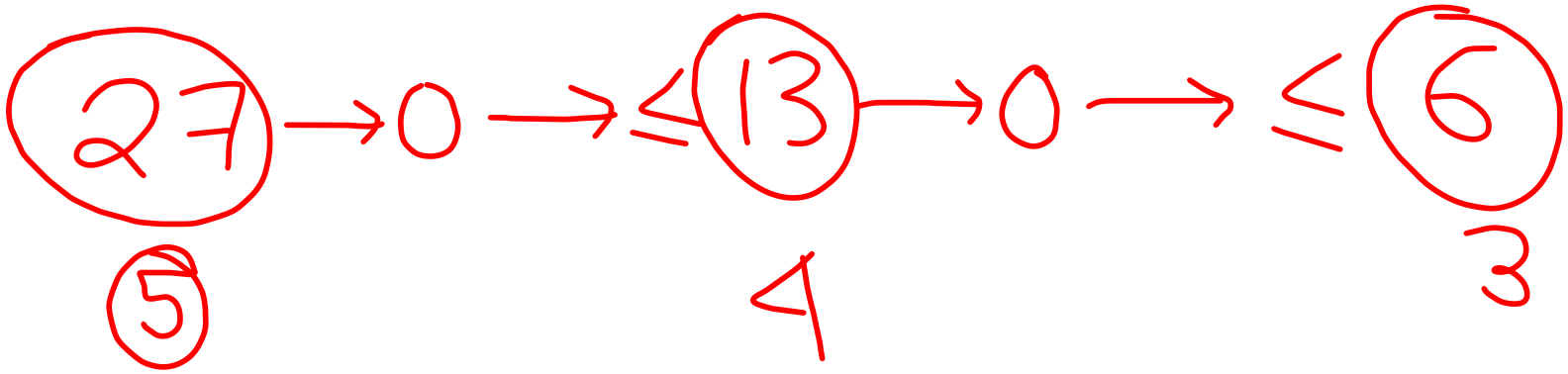
If $b > a/2$. $[a \bmod b] = a - b < a/2$

Fix integer i, $0 \le i \le k-2$.

Consider the execution of $(i+2)^{\text{th}}$ call to GCD

$$b_{i+2} = (a_{i+1} \bmod b_{i+1}) < \frac{a_{i+1}}{2} = \frac{b_i}{2}$$

Corollary: In an execution of alg GCD(a, b), there are at most 2||b||-2 recursive calls. Note that ||b|| denotes the length of "b" in bits



Let $d = gcd(a, b)$

$d = aX + bY$ for some $X, Y \in \mathbb{Z}$.

Extended Euclidean algorithm:

Input $a, b : a, b \in \mathbb{Z}, b > 0$

Output: (d, X, Y) where $d = gcd(a,b)$ and $d = aX + bY$.

Base Cond^n:

If $b \mid a$ then return $(b, 0, 1)$

Else

$(d, X, Y) \leftarrow eGCD(b, a \bmod b)$

Let $d = gcd(a, b)$

$d = aX + bY$ for some $X, Y \in \mathbb{Z}$.

Extended Euclidean algorithm:

Input $a, b : a, b \in \mathbb{Z}, b > 0$

Output: (d, X, Y) where $d = gcd(a,b)$ and $d = aX + bY$.

Base Cond^n:

If $b \mid a$ then return $(b, 0, 1)$

Else compute q, r such that $a = bq + r$

$(d, X, Y) \leftarrow eGCD(b, r)$

return $(d, Y, X - qY)$

$$d = bx + (a \bmod b)y$$

Let $r = a \bmod b$

$\Rightarrow r = a - bq$ for some $q \in \mathbb{Z}$.

$$\begin{aligned} d &= bx + ry \\ &= bx + (a - bq)y \\ &= bx + ay - bqy \\ &= \underbrace{ay}_{x'} + b\underbrace{(x - qy)}_{y'} \end{aligned}$$

Example:

gcd(27, 12)

3 = gcd(27, 12)

3 = 27·x + 12·y

= 27·1 + 12·(−2)

27 = 12·2 + 3

q r

(3, 1, −2)

x y

eGCD(27, 12)

↓

eGCD(12, 3)

(3, 0, 1)

↓ ↓

x y

3 = 12·0 + 3·1

x y

x = 1, y = −2.

Suppose N is an integer.

Let $a \in \mathbb{Z}_N$.

Determine whether $a \in \mathbb{Z}_N^*$

$\gcd(a, N) \stackrel{?}{=} 1$ X and Y such that $aX + NY = 1$ ← inverse of a modulo N.

b is said to be inverse of a modulo N if

$ab \equiv 1 \bmod N$.

$\Rightarrow (ab - 1) = kN \Rightarrow ab - kN = 1$

Modular Multiplicative Inverse:

Input: some modulus N. and some $a \in \mathbb{Z}_N$

output: Inverse of a modulo N.

Compute $(d, X, Y) \leftarrow eGCD(a, N)$

If $d \neq 1$ then return multiplicative inverse does not exist

else return X.