Cor. $a = \prod p_i^{a_i}$, $b = \prod p_i^{b_i}$

$$\gcd(a,b) = \prod p_i^{\min(a_i, b_i)}$$

An algorithm for gcd

factor a (into primes)

factor b

take min of exponents

$a = n$ bit #

Factoring (a)

For $d = 2, 3, 4, 5 \cdots \cancel{a-1}$ $\sqrt{a}$ a/a

see if $d \mid a$

if so continue on $\frac{a}{d}$ starting with d

2^n trial divisions

$n = 32 \to$ 4 billion

$n = 64 \to$ 16 billion billion

10^{25}

if $a = x \cdot y$ then either $x \leq \sqrt{a}$ or $y \leq \sqrt{a}$

$n = 1000$

$2^{1000} \sim 10^{300}$

(if not $x \cdot y > \sqrt{a} \cdot \sqrt{a} = a$)

$\sim 10^{80}$ atoms in universe

With $\sqrt{a}$ optimization

$\sim 2^{n/2}$ $\quad 2^{1000/2} = 2^{500} = 10^{150}$

GCD(a, b)
while b ≠ 0 {
r = a mod b
a = b
b = r }
return a

Euclid's algorithm < 300 BC

a = 440 b = 300

$$\overset{a}{440} = 1 \cdot \overset{b}{300} + \overset{r}{140}$$

$$300 = 2 \cdot 140 + 20$$

$$140 = 7 \cdot 20 + 0$$

20   $\underline{0}$

→ gcd = 20

let $a = q\,b + r$ $\quad 0 \le r < b$

q: quotient, r: remainder

<u>claim</u> $\gcd(a, b) = \gcd(b, r)$

---

if $d \mid a$ & $d \mid b$

then $d \mid a + b$

and $d \mid sa + tb \quad \forall s, t \in \mathbb{Z}$

$d \mid a \Rightarrow \exists\ u$ st $a = du$

$d \mid b \Rightarrow \exists\ v$ st $b = dv$

$sa + tb = sdu + tdv$

$= d(su + tv)$

$\therefore d \mid sa + tb$

$a = qb + r$

if <u>$d \mid a$ & $d \mid b$</u> then $d \mid r$ since $r = a - bq$