while $b \neq 0$
$r = a \bmod b$
$a = b$
$b = r$

Claim: b gets shorter by at least 1 bit every 2 iterations

$\therefore$ Time $O(n)$ (length of b in bits)

vs $2^{n/2}$ by factoring method from Wednesday.

Case 1:

$r \leq b/2$

Case 2:

$r > b/2$

in next iteration, $q = 1$

~~so~~ new $r = b - \text{old } r$

$\leq b/2$

Theorem $\forall a, b > 0\ \exists s, t \in \mathbb{Z}$

s.t. $sa + tb = \gcd(a, b)$

proof by example

$440 = 300 \cdot 1 + 140$ $\qquad 140 = 440 - 1 \cdot 300$

$300 = 140 \cdot 2 + \underline{20}$ $\qquad 20 = 300 - 2 \cdot 140$

$140 = 7 \cdot 20 + 0$ $\qquad = 300 - 2(440 - 300)$

$\qquad = 3 \cdot 300 - 2 \cdot 440$

$6, \cancel{5}35$ $\qquad \gcd(6, 35) = 1$

$2 \cdot 3 \quad 7 \cdot 5$

$6 \cdot 6 - 1 \cdot 35 = 1$

---

if $a \mid bc$ does $a \mid b$?

or $a \mid c$

$2 \cdot 3 \mid 4 \cdot 9$

$6 \mid \cancel{36}\ 4 \cdot 9$

Theorem

if $a \mid b \cdot c$ & $\gcd(a,b) = 1$ then $a \mid c$

Pf

$\exists\, s,t \quad sa + tb = 1$

$sac + tbc = c$

$a \mid sac$

$a \mid bc$ so $a \mid tbc$

$\therefore\ a \mid (sac + tbc)$

$\therefore\ a \mid c$

if prime $p \mid \prod_{i=1}^{n} q_i$

Then $\exists$ j st. $p \mid q_j$

pf by ind on n

if $p \mid q_1$ done

if not $\gcd(p, q_1) = 1$

by previous theorem $p \mid \prod_{i=2}^{n} q_i$

by ind $p \mid q_j$ for some j.

---

uniqueness of prime factorization

suppose not. Let n be smallest exception

$$p_1 \cdot p_2 \cdots p_s = n = q_1 q_2 \cdots q_t$$

$p_1 = q_j$ for some j

$$p_2 \cdot p_3 \cdots p_s = \frac{n}{p_1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_t$$

contradicting minimality of n.