(Continued from last class...)

GCDWR

If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

Proof: If $a = b = 0$, then since $r = a - bq$, $r = 0$. Hence $\gcd(a, b) = 0 = \gcd(b, r)$. Thus, assume that $a \neq 0$ or $b \neq 0$.

Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$

Since $a = bq + r$ and $d \mid a$ and $d \mid b$

By DIC $d \mid a - bq = r$. Thus,

$d \leq e$ (1) since e is the largest divisor of b & r. Now, $e \mid b$ and $e \mid r$ so by DIC $e \mid bq + r = a$. Thus $e \leq d$ (2) since d is the largest common divisor of a & b. By (1) and (2) $d = e$. ☐

Prove that $\gcd(3a+b, a) = \gcd(a, b)$ using GCDWR.

"a" "q" "b" "r"

$3a+b = (3)a + b$

GCDWR $\Rightarrow$ $\gcd(\text{"a"}, \text{"b"}) = \gcd(\text{"b"}, \text{"r"})$

$\gcd(3a+b, a) = \gcd(a, b)$

Euclidean Algorithm

Idea: Compute GCDs quickly by using GCD WR & Division Algorithm.

Ex: Compute gcd(1239, 735)

(01) $1239 = 735(1) + 504$ (1)

$735 = 504(1) + 231$ (2)

$504 = 231(2) + 42$ (3)

$231 = 42(5) + 21$ (4)

$42 = 21(2) + 0$

Thus, by GCDWR,

$\gcd(1739, 735) = \gcd(735, 504)$

$= \gcd(504, 231) = \gcd(231, 42)$

$= \gcd(42, 21) = \gcd(21, 0) = 21$

NB: This process stops ∵ remainders form a sequence of non-negative decreasing integers.

Q: What is the runtime of Euclidean Alg'm?

Back Substitution

Q: Do there exist integers x, y s.t. $ax + by = \gcd(a, b)$? A: YES!

$21 = 231 + 42(-5)$ (by (4))

by (3) $= 231 + (504 + 231(-2))(-5)$

$= 231(11) + 504(-5)$

by (2) $= (735 + 504(-1))(11) + 504(-5)$

$= 735(11) + 504(-16)$

by (1) $= 735(11) + (1239 + 735(-1))(-16)$

$= 735(27) + 1239(-16)$.

Use the Euclidean Algorithm to compute $\gcd(120, 84)$ and then use back substitution to find integers x and y such that $\gcd(120, 84) = 120x + 84y$.

$120 = 84(1) + 36$ By E.A. &

$84 = 36(2) + 12$ GCDWR.

$36 = 12(3) + 0$ $\gcd(120, 84) = 12$.

. . . .

$12 = 84 + 36(-2)$

$= 84 + (120 + 84(-1))(-2)$

$= 84(3) + 120(-2)$

$84(3 + 120) + 120(-2 \cdot 84)$

$84 \cdot 3 = 252$

$120 \cdot (-2) = -240$

12 ✓

Bézout's Lemma (GCDCT in the notes)

Let $a, b \in \mathbb{Z}$ then

(i) If $d = \gcd(a,b)$ then $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = d$.

(ii) If $d > 0$, $d|a$, $d|b$ and $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = d$ then $d = \gcd(a,b)$

Pf: (i) Painful. Use Back Substitution

(ii) Let $e = \gcd(a,b)$. Since $d|a \wedge d|b$ by maximality, $d \leq e$. Now, $e|a \wedge e|b$ so by DIC, $e | ax+by = d$. So by BBD, $|e| \leq |d|$ and $\because e, d > 0$ $e \leq d$. Thus, $d = e$. ∎