Discrete Math

Lecture 31

# The Division "Algorithm" (& Friends)

## The Div "Alg"

$a, b$ + $b \neq 0$

$$a = q \cdot b + r$$

$$0 \leq r < |b|$$

## Greatest Common Divisor

gcd

$a, b \in \mathbb{Z}$ (not both $= 0$)

$\gcd(a,b)$ = the largest positive integer that divides both

i.e. $d = \gcd(a,b)$ means:

$$d \mid a, \quad d \mid b$$

if $c \mid a \wedge c \mid b$ then $c \leq d$

ex) $a = 28, \quad b = 16$

$$D_+(a) = D_+(28) = \{1, 2, 4, 7, 14, 28\}$$

$$D_+(b) = D_+(16) = \{1, 2, 4, 8, 16\}$$

$$D_+(28) \cap D_+(16) = \{1, 2, 4\}$$

$4 \leftarrow \gcd(28, 16)$

ex) $\gcd(1044, 339)$.

writing out all divisors of (moderately) big integers is tedious or difficult!

Euclid's Division Algorithm (compute gcd)

**Euclidean Algorithm**

(1) Given $a, b \in \mathbb{Z}$ with $b \neq 0$, use the Division "Algorithm" to write

$a = q_1 \cdot b + r_1$

(2) Apply the Division "Algorithm" to $b$ and $r_1$ to find

$b = q_2 \cdot r_1 + r_2$

(3) Repeatedly apply the Division "Algorithm" until a remainder with value 0 is produced

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \\
b &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
r_2 &= q_4 \cdot r_3 + r_4 \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + \boxed{r_n} \\
r_{n-1} &= q_{n+1} \cdot r_n + 0
\end{aligned}$$

(4) If $r_{n+1} = 0$, then the previous remainder, $r_n$, is the $\gcd(a, b)$.

gcd(1044, 339) use Euclid's Algorithm

$$1044 = \underline{3} \cdot 339 + \underline{27}$$

$$339 = \underline{12} \cdot 27 + \underline{15}$$

$$27 = \underline{1} \cdot 15 + \underline{12}$$

$$15 = \underline{1} \cdot 12 + \underline{3}$$

$$12 = \underline{4} \cdot 3 + \underline{\boxed{0}}$$

gcd(1044, 339)

Why does Euclid's Alg. produce the gcd?

two key reasons

- $\gcd(c, 0) = c$

why? $D_+(0) = \{1, 2, \ldots c \ldots\}$ $D_+(c) = \{1, \ldots, c\}$

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

$$= \gcd(a-2b,\ b)$$

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

$$\vdots$$

$$= \gcd(a-qb,\ b)$$

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

$$\boxed{\gcd(a,b) = \gcd(b,r)}$$

$$\vdots$$

$$= \gcd(d,0) = d$$

# Bezout's Identity

$\forall\ a, b \in \mathbb{Z},\ \exists\ x, y \in \mathbb{Z},$

$$\underbrace{ax + by}_{\text{an integer linear combo. of } a \,\&\, b} = \gcd(a,b)$$

- coefficients $x, y$ are not unique
- you can find values for $x$ & $y$ using the Euclidean Alg. backwards!

**Example 3.2.** *We recall the steps from the Euclidean Division Algorithm used to compute* $\gcd(120, 34) = 2$*:*

$$120 = 3 \cdot 34 + 18$$
$$34 = 1 \cdot 18 + 16$$
$$18 = 1 \cdot 16 + 2$$
$$16 = 8 \cdot 2 + \boxed{0}$$

Beginning with the second to the last line, we can solve for 2 = gcd(120, 34) to

$$2 = 120 \cdot x + 34 \cdot y$$

$18 = 1 \cdot 16 + 2 \longrightarrow 2 = 18 - 1 \cdot 16$

$34 = 1 \cdot 18 + 16$

$\downarrow$

$16 = 34 - 18$

$$2 = 18 - (34 - 18)$$

$$2 = 2 \cdot 18 - 34$$

$120 = 3 \cdot 34 + 18$

$\downarrow$

$18 = 120 - 3 \cdot 34$

$$2 = 2 \cdot (120 - 3 \cdot 34) - 34$$

$$2 = 2 \cdot 120 - 6 \cdot 34 - 34$$

$$2 = \underset{x}{\underset{\uparrow}{2}} \cdot 120 + \underset{y}{\underset{\uparrow}{(-7)}} \cdot 34$$

✓ ✓

**Def** If $\gcd(a,b) = 1$

then we say a + b are

**relatively prime**

**ex** $\gcd(121, 49) = 1$

121 + 49 are relatively prime

**Bezout's Id.** $\exists\, x, y,\ 121 \cdot x + 49 \cdot y = 1$

_ _ _ _ _ _ _