Greatest Common Divisor

DEF: For integers a, b not both 0, the greatest common divisor of a and b is the largest positive d s.t. $d \mid a$ and $d \mid b$

$\gcd(6, 21) = 3$

$\gcd(28, 144) = 4$

$\gcd(24616, 15678) = 2$

$2 \cdot 2 \cdot 2 \cdot 17 \cdot 181 \qquad 2 \cdot 3 \cdot 3 \cdot 13 \cdot 67$

$\gcd(1040279, 1034273) =$

$1007 \cdot 1031$

$$\frac{24616}{2} \qquad \underline{12308}$$

THM: For any integers a, b, q, r, if $b \neq 0$ and $a = b \cdot q + r$, then $\gcd(a,b) = \gcd(b, r)$

gives Euclidean algorithm for computing $\gcd(a,b)$:

compute $q = a \text{ div } b$
$r = a \bmod b$

repeat with new a = b, new b = r until new b = r = 0

$\gcd(24616, 15678) = \gcd(15678, 8938)$ $\quad 24616 = 1 \cdot 15678 + 8938$

$= \gcd(8938, 6740)$ $\quad 15678 = 1 \cdot 8938 + 6740$

$= \gcd(6740, 2198)$ $\quad 8938 = 1 \cdot 6740 + 2198$

$= \gcd(2198, 146)$ $\quad 6740 = 3 \cdot 2198 + 146$

$= \gcd(146, 8)$ $\quad 2198 = 15 \cdot 146 + 8$

$= \gcd(8, 2)$ $\quad 146 = 18 \cdot 8 + 2$

$= \gcd(2, 0)$ $\quad 8 = 4 \cdot 2 + 0$

$\boxed{= 2}$

$\gcd(a, 0) = a$
for any positive $a \in \mathbb{Z}$

Proof: Let a, b, q, r be integers such that $b \neq 0$ and $a = b \cdot q + r$.

We show a) $\gcd(a,b) \leq \gcd(b,r)$

let $d = \gcd(a,b)$. By def gcd,
$d \mid a$ and $d \mid b$.
$r = a - bq$ where $d \mid a$ and $d \mid bq$
and so $d \mid a - bq$ iow $d \mid r$.
So d is a common divisor of b and r
By def gcd $\gcd(b,r) \geq d = \gcd(a,b)$

find d s.t.
$d \mid b$ and $d \mid r$
so d is a common divisor of b, r
and $\leq \gcd(b,r)$

to show a = b
it suffices to show $a \leq b$
and $b \leq a$

and b) $\gcd(b,r) \leq \gcd(a,b)$

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

on PSet 4

and therefore $\gcd(a,b) = \gcd(q,r)$

Induction

if it rains one day then

it will rain the next

we land ... it is raining

was it raining the day before?

???

$P(n)$ = "it is raining on day n"

will it rain tomorrow? Y

and the next Y

and the next Y

it will rain from now on

base case

$P(0)$

$P(0) \to P(1)$ ✓

$P(1) \to P(2)$ ✓✓

$P(2) \to P(3)$ ✓✓

$\vdots$

$\therefore \forall n \in \mathbb{Z}, n \geq 0 \to P(n)$

$\forall n \in \mathbb{Z}, n \geq 0 \to (P(n) \to P(n+1))$ induction step

$P(3)$

Principle of Mathematical Induction

If $P(0)$ is true and $\forall k \in \mathbb{Z}, k \geq 0 \wedge P(k) \to P(k+1)$ is true, then $\forall n \in \mathbb{Z}, n \geq 0 \to P(n)$

If $P(a)$ is true and $\forall k \in \mathbb{Z}, k \geq a \wedge P(k) \to P(k+1)$ is true, then $\forall n \in \mathbb{Z}, n \geq a \to P(n)$

Summations

$\sum_{i=1}^{0} a_i$ is empty sum defined to be 0

$\prod_{i=1}^{10} 3i = 3 \cdot 6 \cdot 9 \cdots \cdot 30$

$\bigwedge \quad \bigvee$

$\underset{i=n}{\oplus} a_i$

$a_0, a_1, a_2, \ldots$ is a sequence

Define seq a by $a_i = \underline{3i-9}$ for $i \geq 0$ $\quad a_0 = -9 \quad a_1 = -6 \quad a_2 = -3$

$\underline{-9, -6, -3, 0, 3, \ldots}$

$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$

$= -6 + -3 + 0 + \cdots + (3n-9)$

$\overbrace{1 + \underbrace{2 + \overbrace{\cdots}{} + (n-1)}_{\frac{n}{2}(n+1)} + n}$ implicitly defines $a_i = i$

n		
1	1	1
2	1+2	3
3	1+2+3	6

$1+2+3+\cdots+n$

THM: For any integer $\underline{n \geq 0}$, $\boxed{\sum_{i=1}^{n} i = \frac{n(n+1)}{2}}$ P(n)

Proof: (By induction)

Base case (n=0): $\sum_{i=1}^{0} i = 0$ by def of empty sum $\quad P(0) = \sum_{i=1}^{0} i = \frac{0(0+1)}{2}$

$\frac{0(0+1)}{2} = 0$

so $\sum_{i=1}^{0} i = \frac{n(n+1)}{2}$ since both $= 0$

$P(0) \to P(1)$
$P(1) \to P(2)$
$P(2) \to P(3)$
$\vdots$

Ind step: [want $\forall k \geq 0$, $\boxed{P(k) \to P(k+1)}$] $\quad$ P(k) Ind. hypothesis

Suppose $k \in \mathbb{Z}$ s.t. $k \geq 0$ and $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

[want: $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$] P(k+1)

Then $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$

$= \frac{k(k+1)}{2} + k+1 = \frac{k(k+1)}{2} + \frac{2(k+1)}{2}$

$= \frac{k(k+1) + 2(k+1)}{2}$

$= \frac{(k+1)(k+2)}{2}$ $\ddot\smile$

$r = \frac{1}{2} \quad (\frac{1}{2})^0, (\frac{1}{2})^1, (\frac{1}{2})^2, \ldots \quad \frac{(\frac{1}{2})^5 - 1}{\frac{1}{2} - 1} \quad \frac{\frac{-31}{32}}{-\frac{1}{2}}$

$= \underset{a_0}{1}, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \underset{a_4}{\frac{1}{16}}, \ldots \ldots \quad 1\frac{15}{16}$

geometric sequence

THM: For any real number $r \neq 1$ and integer $n \geq 0$, $\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$ P(n)

$\forall r, r \neq 1, \forall n \in \mathbb{Z}, n \geq 0 \to$

Proof: Suppose r is a real number with $r \neq 1$.

Prove $\forall n \in \mathbb{Z}$ $n \geq 0 \to \underbrace{\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}}$ by induction

Base case (n=0) $\sum_{i=0}^{0} r^i = r^0 = 1$ $\quad P(0) = \sum_{i=0}^{0} r^i = \frac{r^1 - 1}{}$

Prove $\forall n \in \mathbb{Z}\ n \geq 0 \Rightarrow \underbrace{\sum_{i=0} r^{i} = \frac{1}{r-1}}$ by induction

Base case $(n=0)$ $\sum_{i=0}^{0} r^i = r^0 = 1$

$\frac{r-1}{r-1} = 1$

=

$P(0) = \sum_{i=0}^{0} r^i = \frac{r^1-1}{r-1}$

Ind step: Suppose $k \geq 0$ and $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$ [want: $\sum_{i=0}^{k+1} r^i = \frac{r^{k+2}-1}{r-1}$]

Then $\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1}$

$= \frac{r^{k+1}-1}{r-1} + r^{k+1}$

$= \frac{r^{k+1}-1 + (r-1)r^{k+1}}{r-1}$

$= \frac{\cancel{r^{k+1}}-1 + r^{k+2} \cancel{-r^{k+1}}}{r-1}$

$= \frac{r^{k+2}-1}{r-1}$

$\sum_{i=1}^{n}(6i-4)$

$= \sum_{i=1}^{n} 6i - \sum_{i=1}^{n} 4$

$= 6\sum_{i=1}^{n} i - 4n$

Pierogies

Yocco's sells pierogi in orders of 3, 4, and 7.

Can you order exactly 5 pierogi? N

6	3+3	Y
7	7	Y
8	4+4	Y
9	3+3+3	Y
10	3+7	Y
		⋮

THM: For all integers $n \geq 6$, $\exists a,b,c \in \mathbb{N}$ s.t. $n = 3a+4b+7c$.

Proof: