Thm: All strategies for the n-block games produce the same score $S(n)$. $=\frac{n(n-1)}{2}$

ex) $S(8)=28$

pf. By strong induction

I.H: $P(n)=$ All strategies for the n-block games produce the same score $S(n)$.

Basecase: $n=1$, $S(1)=0$ ✓ $S(1)=\frac{1\cdot 0}{2}=0$

Inductive step: Assume $P(1), P(2) \cdots P(n)$ to prove $P(n+1)$. Look at $n+1$ blocks $\begin{array}{c} n+1 \\ \swarrow \quad \searrow \\ k \quad\quad n+1-k \end{array}$, $1 \le k \le n$

$S(n+1)$

Score $= k(n+1-k)+P(k)+P(n+1-k)$ → depends on k. Need a stronger induction hypothesis.

$$=k(n+1-k)+\frac{k(k-1)}{2}+\frac{(n+1-k)(n+1-k-1)}{2}=\frac{\cancel{2kn}+\cancel{2k}-\cancel{2k^2}+\cancel{k^2}-\cancel{k}+(n+1)n-\cancel{kn}-\cancel{k}-\cancel{kn}+\cancel{k^2}}{2}=\frac{n(n+1)}{2}=S(n). \square$$

Number Theory

Number Theory: Study of integers

Def. $m|a$ (m divides a) iff $\exists k$ $a=k\cdot m$

$m|0$ for all integers ($a=0=0\cdot m$)

Suppose we have a gallon jug and b gallon jug, $a \le b$

Thm. If $m|a$ & $m|b$, then $m|$(any results from the transitions)

<u>State machine</u>

States, pairs (x,y), where $x=$ # of gallons in the a jug

$y=$ # of gallons in the b jug

Start-State: $(0,0)$

Transitions: * emptying ex) $(x,y)\to(0,y)$, $(x,y)\to(x,0)$

* filling ex) $(x,y)\to(x,b)$, $(x,y)\to(a,y)$

* pouring ex) $(x,y)\to(0,x+y)$, $x+y\le b$, $(x,y)\to(x-\underbrace{(b-y)}_{\text{space left in b jug}},b)=(x+y-b,b)$, $x+y\ge b$

$(x,y)\to(x+y,0)$, $x+y\le a$, $(x,y)\to(a,y-(a-x))=(a,x+y-a)$, $x+y\ge a$

ex) $a=3, b=5$, trying to get 4 gallons

Starts with $(0,0) \to (0,5) \to (3,2) \to (0,2) \to (2,0) \to (2,5) \to (3,4)$

pf. (by induction) Assume $m|a$ & $m|b$

Invariant: $P(n)$ = "If (x,y) is the state after n transitions, then $m|x$ & $m|y$"

<u>Basecase</u>: $(0,0)$, $m|0$ for all integers $\Rightarrow P(0)$ ✓

<u>Inductive Step</u>: Assume $P(n)$ to prove $P(n+1)$

Suppose that (x,y) is the state after n transitions. $P(n) \Rightarrow m|x$ and $m|y$

After another transition, each of the Jugs are filled with $0 \vee a \vee b \vee x \vee y \vee x+y \vee x+y-a \vee x+y-b$ gallons.

We know that $m|0, m|a, m|b, m|x, m|y \Rightarrow m$ divides any of the above because $x+y, x+y-a, x+y-b$ are all linear combinations of $0, a, b, x, y \Rightarrow P(n+1)$ ✓

ex) $a=33, b=55$, trying to get 4 gallons $\Rightarrow$ impossible

Because a and b are both divisible by 11, the results from the transition must be divisible by 11 but 4 is not.

Def: $\gcd(a,b)$ = the greatest common divisor of a and b

ex) $\gcd(52,44)=4$

Def. We say that a and b are relatively prime if $\gcd(a,b)=1$

Thm. If $m|a$ & $m|b$, then $m|$(any results from the transitions)

Corollary. $\gcd(a,b)|$(any results from the transitions)

Thm. Any linear combination $L = s \times a + t \times b$, of a and b (s, t are integers) with $0 \le L \le b$ can be reached. ($b \ge a$)

$$\begin{array}{rl} 4 = & (-2)\cdot 3 + 2\cdot 5 \\ & \underline{+\,5\cdot 3 - 3\cdot 5} \\ & \underbrace{3}_{s'>0}\cdot 3 - 5 \end{array}$$

pf. Notice $L = sa + tb = \overbrace{(s+mb)}^{s'}a + \overbrace{(t-ma)}^{t'}b$. So, $\exists s', t'$ s.t $L = s'a + t'b$ with $s' > 0$.

Assume $0 < L < b$

<u>Algorithm</u>: To obtain L gallons we are going to repeat s' times.

- Fill the a-Jug
- Pour into b-Jug. When it becomes full, empty out and continue pouring until a-Jug is empty.

ex) $a = 3, b = 5$

First loop: $(0,0) \to (3,0) \to (0,3)$

Second loop: $(0,3) \to (3,3) \to (1,5) \to (1,0) \to (0,1)$

Third loop: $(0,1) \to (3,1) \to (0,4)$

Filled the a-Jug s' times. Suppose that b-Jug is emptied u times. Let r be the remainder in the b-Jug.

$0 \le r \le b$ $\quad$ $0 < L < b$

$r = s' \cdot a - u \cdot b$ $\quad$ $L = s'a + t'b$

$r = \overbrace{s'a + t'b}^{L} - t'b - u \cdot b = L - (t' + u)b.$

If $(t' + u) \ne 0 \Rightarrow [r < 0 \vee r > b]$: this cannot be the case.

If $(t' + u) = 0 \Rightarrow u = -t' \Rightarrow r = s' \cdot a - (-t')b = s'a + t'b = L$

$\gcd(3,5) = 1$, $1 = 2\cdot 3 - 1\cdot 5$

There exists a unique q (quotient) and $\underset{\text{rem}(b,a)}{r}$ (remainder) s.t $b = qa + r$ with $0 \le r < a$

<u>Lemma</u> $\gcd(a,b) = \gcd(\text{rem}(b,a), a)$

ex) $\gcd(105, 244) = \gcd(\text{rem}(244, 105), 105) = \gcd(\text{rem}(244, 105), 105) = \gcd(14, 105) = \gcd(\text{rem}(105, 14), 14) = \gcd(7, 14) = \gcd(\text{rem}(14, 7), 7) = \gcd(0, 7) = 7$

$224 = 2\cdot 105 + 14$ $\quad$ $105 = 7 \times 14 + 14$

$\Rightarrow$ Euclid's Algorithm

pf for Lemma $gcd(a,b) = gcd(rem(b,a),a)$

$[m|a \wedge m|b] \Rightarrow [m|b-qa=rem(b,a) \wedge m|a]$

If $rem(b,a) \neq 0$ then $[m|rem(b,a)=b-qa$ and $m|a] \Rightarrow [m|a \wedge m|b]$ (because $b-qa+a \times q=b$ (can be obtained by linear combination))

If $rem(b,a)=0=b-qa \Rightarrow b=qa, m|a \Rightarrow m|b$ because $b=qa$ is linear combination of a.

Thm. $gcd(a,b)$ is a linear combination of a and b.

pf. (by induction) Invariant: $P(n)$ = If Euclid's Algorithm reaches $gcd(x,y)$ after n steps, then both x and y are linear combination of a and b, and $gcd(a,b)=gcd(x,y)$

Basecase: $P(0)$ is true because we have taken 0 step, a and b are linear combination of a and b, $gcd(a,b)=gcd(a,b)$

Inductive step: Assume $P(n)$ to show $P(n+1)$

Notice that $\exists q$, $rem(y,x)=y-qx \rightarrow$ linear combination of a and b because x and y are linear combination of a and b.

Therefore, we know that after extra step, what we have reached is still a linear combination of a and b. And the Lemma has shown that the gcd of what we have reached equals to gcd of what we have started with. $\Rightarrow P(n+1)$ ✓

In a very last step of Euclid's Algorithm we achive something of this form $gcd(0,y')=y'$

Thm. $gcd(a,b)$ is the smallest positive linear combination of a and b.