Math 321

~~Q5~~ $p = 53$ $q = 61$ $e = 17$ $\boxed{n = 3233}$ $\boxed{e = 17}$

$m = 3120$

d is e's inverse mod $m = 3120$

$\gcd(3120, 17) =$

$3120 = q \cdot 17 + r$

ex 8

A = 01	H = 08	O = 15	V = 22
B = 02	I = 09	P = 16	W = 23
C = 03	J = 10	Q = 17	X = 24
D = 04	K = 11	R = 18	Y = 25
E = 05	L = 12	S = 19	Z = 26
F = 06	M = 13	T = 20	
G = 07	N = 14	U = 21	

UPLOAD

start @ 1

UP = $\boxed{2116}$

LO = $\boxed{1215}$

AD = 0104 = $\boxed{104}$

start @ 0

UP = $\boxed{2015}$

LO = $\boxed{1114}$

AD = $\boxed{3}$

Blocksize:

AAA
⋮
ZZZ

$E(p) = p^{17} \bmod 3233$ → return a value

0 to 3232

3233 total "symbols"

$26^3 > 3233$ $26^2 < 3233$

$P_1 = 2015$ $C_1 = 2015^{17} \bmod 3233$

decrypt $P_1 = C_1^{d} \bmod 3233$

Ch 5 Induction

$1=2,3,4,\ldots$

Ex) (if $n^2 < 2^n \rightarrow n > 4$) $\equiv$ ($2 \le n \le 4 \rightarrow n^2 \ge 2^n$)

$n=2$
$n=3$ } 3 cases
$n=4$

conjecture: $n = 5, 6, 7, \ldots \rightarrow n^2 < 2^n$

infinite cases

$\forall n\, P(n)$ where U.D. $n = 5, 6, 7, \ldots$

$P(n)$: " $n^2 < 2^n$ "

Past: finite set for n $\quad \forall n P(n) \equiv P(e_1) \land P(e_2) \land \ldots \land P(e_k)$

infinite? $\quad \forall n P(n) \equiv P(e_1) \land P(e_2) \land \ldots$

Ch 5 Induction: technique to prove $\forall n P(n)$ where U.D. is infinite and is a $\boxed{\text{well-ordered}}$ set

$e_1 \le e_2 \le e_3 \le e_4 \le \ldots$

basically there is always a 1st element for any subset of a well-ordered set.

---

goal: $\forall n P(n)$ is true

1. we will use two tautologies to help prove this
2. tautologies are based on well-ordered sets

set $= e_1 \le e_2 \le e_3 \le e_4 \le \ldots$

Tautology #1

$$\boxed{\underbrace{\left[P(e_1) \land \forall k\,(P(e_k) \to P(e_{k+1}))\right]}_{L} \to \underbrace{\forall n\, P(n)}_{R}} \equiv T$$

want T

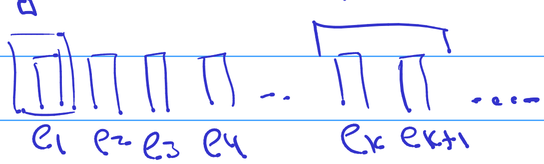
L	R	L → R
T	T	T
~~T~~	~~F~~	~~F~~
F	T	T
F	F	T

→ $\forall n P(n)$ being true is nec. when left is true.

so prove the left $[P(e_1) \land \forall k(P(e_k) \to P(e_{k+1}))]$
show true

$\boxed{\text{case 1}}$ show $P(e_1)$ is true

$\boxed{\text{case 2}}$ show $P(e_k) \to P(e_{k+1})$ is true



Prove by "weak" induction $\forall n\, P(n)$, $n = e_1, e_2, e_3, \ldots$

$\boxed{\text{case 1}}$ (Basis Step) show $P(e_1)$ is true

$\boxed{\text{case 2}}$ ("weak" Inductive Step) show $P(e_k) \to P(e_{k+1})$

2^{nd} tautology:

$$\left[P(e_1) \wedge \forall k \left(P(e_1) \wedge P(e_2) \wedge \dots \wedge P(e_k) \to P(e_{k+1})\right)\right] \to \forall n\, P(n)$$

$\boxed{\text{case 1}}$ (Basis Step) show $P(e_1)$ is true

$\boxed{\text{case 2}}$ (strong inductive Step)
show $(P(e_1) \wedge P(e_2) \wedge \dots \wedge P(e_k)) \to P(e_{k+1})$ is true

---

prove: $\forall n$ " $1+2+\dots+n = \frac{n(n+1)}{2}$ " , $n = 1, 2, 3, \dots$

$P(n)$: " $1+2+\dots+n = \frac{n(n+1)}{2}$ " $n = 1, 2, 3, \dots$

Proof by Induction:

(Basis Step) show $P(e_1)$ is true

$e_1 : n=1$ $\quad P(e_1)$: " $1 = \frac{1(1+1)}{2}$ " true!

(Inductive Step) show $P(e_k) \to P(e_{k+1})$

e_k: $n=k$ $\quad e_{k+1}$: $n=k+1$

$P(n=k)$: " $1+2+\dots+k = \frac{k(k+1)}{2}$ "

$P(n=k+1)$: " $1+2+\dots+(k+1) = \frac{(k+1)(k+2)}{2}$ "