Math 324

Q's: If p is prime then the only solutions to

$$x \cdot x \equiv 1 \pmod{p} \quad (\text{Solve } x^2 \equiv_p 1)$$

are x such that $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$

$\gcd(x, p) = 1 \iff p \nmid x$ (Soln's $x \equiv_p 1$, $x \equiv_p -1$)

$\Rightarrow (1 = s \cdot x + t \cdot p) \bmod p$

$\Rightarrow s \cdot x \equiv 1 \pmod{p}$

Thm: $ac \equiv bc \pmod{n} \wedge \gcd(c, n) = 1 \to a \equiv b \pmod{n}$

$x \equiv 1 \bmod p \qquad x \equiv -1 \pmod{p}$

$x \cdot x \equiv 1 \cdot x \bmod p$

$x^2 \equiv x \pmod{p} \equiv 1 \pmod{p}$

$x \equiv -1 \bmod p$

$x \cdot x \equiv -1 \cdot x \bmod p \equiv 1 \pmod{p}$

So $x \equiv_p 1$ and $x \equiv_p -1$ are solutions.

idea go backwards.

$x^2 \equiv 1 \pmod p$ $\qquad$ $a \equiv b \pmod n$

① $p \mid x^2 - 1$

② $x^2 \bmod p = 1 \bmod p$

③ $x^2 = 1 + k \cdot p$

① $n \mid a - b$

② $a \bmod n = b \bmod n$

③ $a = b + kn$

for some k $\quad k \cdot p = x^2 - 1$

$k \cdot p = (x+1)(x-1) \Rightarrow p \mid x-1 \Rightarrow x \equiv -1 \pmod p$

Something. Prime

$\Rightarrow p \mid x-1 \Rightarrow x \equiv 1 \pmod p$

Short: $x^2 \underset{p}{\equiv} 1 \Rightarrow p \mid x^2 - 1 \Rightarrow p \mid (x+1)(x-1)$

$\Rightarrow p \mid x+1$ or $p \mid x-1$

$\Rightarrow x \underset{p}{\equiv} -1$ or $x \underset{p}{\equiv} 1$

$(9,3,1)_{10}$ to and from $(\ ,\ ,\ )_2$

$(\ ,\ ,\ ,\ ,\boxed{a_i})_b$ $\quad a_i \in \{0,1,\dots,b-1\}$

b^3's b^2's b's 1's

$(9,3,1)_{10}$ $(1,1,1,0,1,0,0,0,1,1)_2$

512's 256's 128's 64's 32's 16's 8's 4's 2's 1's

$9 - 3 = 6$

$512 - 93 = 419$

$419 - 256 = 163$

$163 - 128 = 35$

$35 - 32 = 3$

$(1,0,1,1,1)_2 = 1\cdot 16 + 0\cdot 8 + 1\cdot 4 + 1\cdot 2 + 1 = (23)_{10}$

Induction

$$T \equiv \{[P(1) \wedge \forall k (P(k) \to P(k+1))] \to \forall n P(n)\}$$

1st seq. Notation

$$T \equiv \{[a_1 \wedge \forall k (a_k \to a_{k+1})] \to \forall n\, a_n\}$$

$$T \equiv \{ [P(1) \wedge \forall k((P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \to P(k+1))] \to \forall n P(n) \}$$

What is the purpose of these?

① Common Problem... show $\forall n P(n) \equiv T$

② if $(p \to q) \equiv T$

Means:

p	q	p → q	
T	T	T	①
F	T	T	②
F	F	T	③

SO:

$$\Big(\underbrace{[P(1) \wedge \forall k(P(k) \to P(k+1))]}_{p} \to \underbrace{\forall n P(n)}_{q} \Big) \equiv T$$

want $\forall n P(n) \equiv T$

it is enough to show $\underbrace{P(1)}_{\text{Case 1}} \wedge \underbrace{\forall k (P(k) \to P(k+1))}_{\text{Case 2}} \equiv T$

Weak Induction:

Basis step ① prove $P(1)$

Inductive step ② prove $\forall k\,(P(k) \to P(k+1))$

(ex) Prove: $\forall n\left(1+2+\cdots+n = \frac{n(n+1)}{2}\right)$

Pf: ① Basis (let $n=1$)

$$1 \overset{?}{=} \frac{1(2)}{2}$$

$1 = 1$ yes. (True)

② Inductive Step. $\forall k\,(P(k) \to P(k+1))$ | show!

$P(k)$: $1+2+\cdots+k = \frac{k(k+1)}{2}$ ← assum $P(k)$

$P(k+1)$: $1+2+\cdots+k+(k+1) = \frac{(k+1)(k+2)}{2}$ show $P(k+1)$

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

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

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

So $\forall k(P(k) \to P(k+1))$ is true!

by induction. $\forall n\left(1+\cdots+n = \frac{n(n+1)}{2}\right)$ ☒

Strong Induction:

Basis: $P(1)$

Inductive step: $\forall k\left(P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1)\right)$