Subject: Problem Set 3

Year: Month: Date:

P1

(a) skip. $7 \cdot 135 - 16 \cdot 59 = 1$

(b) ~~123. 135~~ $135 - 16 = 119$

(c) 17^{29}.

(d) $82248 \div 81$

$\cancel{17 \overset{31}{\equiv} 17}$

$\cancel{17^2 \overset{31}{\equiv} 289 \equiv 10}$

$\cancel{17^4 \overset{31}{\equiv} 100 \equiv 7}$

$\cancel{17^8 \overset{31}{\equiv} 18}$

$\cancel{17^{16} \overset{31}{\equiv}}$

P2 (a) $b = ak \rightarrow bc = a(kc)$

(b) $b = ak \wedge c = ak' \rightarrow sb + tc = s(ak) + t(ak')$

(c) $b = ak \Leftrightarrow bc = akc \Leftrightarrow$ Problem Statement

(d) $ik_a + jkb = \cancel{d}\, k \underbrace{(ia + jb)}_{\text{smallest by \#}}$

P3(a) $x^2 - y^2 = (x-y)(x+y)\ \cancel{p}$

$\Rightarrow \underbrace{(x-y)}\underbrace{(x+y)} \mid p \Rightarrow$

V

(b) $n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ ✓

(c) $n^{\frac{4k+3+1}{2}} \equiv n^{2k+2} \equiv n^{\frac{p+1}{2}} \equiv x^{p+1} \equiv x$

P4. $\left|\{mp \mid m \in [0, p^{k-1}-1]\}\right| = p^{k-1}$

P5.

(a) Proof (by Induction).

I.H. $P(n) ::=$ after n steps all numbers on the board can be divided by $\gcd(a,b)$.

B.C. $\gcd(a,b) \mid a, b$ $\quad P(0)$ ✓

I.S. after n steps. the n+1st number is called m.

case 1. m is a divider of both of a or b selected as → (WLOG) $m \mid a \wedge m \mid b$

therefor → $m \mid sa+tb = gcd$

Subject: Year: Month: Date:

Case2 $a \neq x$ or $b \neq y$

by $P(n)$ (WLOG) $m | a, a | gcd$

$\rightarrow m | gcd$

(b) Proof by contradiction

d is not on board $\rightarrow d | gcd$

$\rightarrow d | a, b \rightarrow$ game not over. $\#$

(c) calculate number $|\{d \mid d | gcd\}|$

P6

(a) Proof by contradiction.

$F = \{P_1, \dots, P_k\} \rightarrow n = P_1 \cdot P_2 \cdots P_k + 1$

$\rightarrow P_{1 \dots n} \nmid n \rightarrow \#$

(b) Proof by C.A.

$P \equiv 0$ $\#$ $2 | P$

$P \equiv 2 \rightarrow P = 4k+2 \rightarrow 2 | P$ $\#$

Subject:　　　　　　　　Year:　　Month:　　Date:

(c) Proof by contradiction

$\forall p,\ p \overset{4}{\not\equiv} 3 \to p = 2$ ※

$\quad \hookrightarrow p \overset{4}{\equiv} 1 \to n \overset{4}{\equiv} 1$ ※

(d) Proof by ※

assume $F = \{p_1 \cdots p_n\}$ is finite

$F = \{p \mid p \overset{4}{\equiv} 3\}$

suppose $n = 4p_1 \cdots p_n - 1$

$\to \exists p_i,\ p_i \mid n$

$\to \nexists \forall p_i,\ n \overset{p_i}{\equiv} -1 \to$ ※