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) $82248 \div 81$ $17^2 \equiv 289 \equiv 10$

$17^4 \equiv 100 \equiv 7$

$17^8 \equiv 18$

$17^{16} \equiv$

P2 (a) $b = qk \rightarrow bc = q(kc)$

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

(c) $b = qk \Leftrightarrow bc = qkc \Leftrightarrow$ Problem Statement

(d) $ikq + jkb = k(iq + jb)$

smallest by def

P3(a) $x^2 - y^2 = (x-y)(x+y)$

$\Rightarrow (x-y) \mid (x+y) \mid P \Rightarrow$

V

Subject: Year: Month: Date:

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

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

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. $gcd(a,b) \mid a, b$ $P(0)$ ✓

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

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

therefor ~~[illegible]~~ → $m \mid sa + tb = gcd$

Subject: Year: Month: Date:

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

by P(n) (WLOG) $m \mid a, a \mid gcd$

$\rightarrow m \mid gcd$

(b) Proof by contradiction

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

$\rightarrow d \mid a \wedge b \rightarrow$ game not over. ※

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

Pf

(a) Proof by contradiction.

$F = \{p_1, \ldots, p_k\} \rightarrow n = p_1 \cdot p_2 \cdots p_k + 1$

$\rightarrow p_{1 \ldots n} \nmid n \rightarrow$ ※

(b) Proof by C.A.

$P \equiv 0$ ※ $2 \nmid P$

$P \equiv 2 \rightarrow P = 4k+2 \rightarrow 2 \mid P$ ※

Subject:

Year: Month: Date:

(c) Proof by contradiction

$\forall P,\ P \overset{4}{\not\equiv} 3 \rightarrow P = 2$ ※

$\quad \rightarrow P \overset{4}{\equiv} 1 \rightarrow h \overset{4}{\equiv} 1$ ※

(d) Proof by ※

assume $F = \{P_1 \cdots P_n\}$ is finite

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

Suppose $h = 4P_1 \cdots P_n - 1$

$\rightarrow \exists P_i,\ P_i \mid h$

$\rightarrow \cancel{\forall} P_i,\ h \overset{P_i}{\equiv} -1 \rightarrow$ ※