Problem 1.

(a)

x	y	$rem(x,y)=x-q.y$
135	59	17 = 135-2*59
59	17	8 = 59 - 3*17 8 = -3*135 + 7* 59
17	8	1 = 17-2*8
8	1	0 = 8-8*1

last none zero remainder is 1 , then:

$1=17-2*8$
$1=(135-2*59)-2(7*59-3*135)$
$1=7*135-16*59$ #

(b)

from part (a)

$59\cdot k\equiv 1(mod\,135)$
$-16*59\equiv 1(mod\,135)$ by adding a cycle
$119*59\equiv 1(mod\,135)$ #

(c)

$rem(17^{29},31)$

by factoring $17^{29}=17^{1}+17^{4}+17^{8}+17^{16}$

$17^{2}=289$ $17^{4}=10^{2}$ $17^{8}\equiv 18$ $17^{16}\equiv 14$

$17^{2}\equiv 10$ $17^{4}\equiv 7$

so $17^{19}\equiv 17*18*7*14$
$17^{19}\equiv 11$

Problem 2.

(a) since $a|b$ then there exists integer k such that $ak=b$, multiplying both sides by c resulting that $akc=bc$ can rewritten as $a(kc)=bc$ implying that $a|bc$.

(b) since a divides b, then there exists integer $ak_1=b$ same for c, $ak_2=c$, then we can rewrite $a|sb+tc$ as $a|s(ak_1)+t(ak_2)$ by rearranging $a|a(sk_1+tk_2)$ which is true.

(c) since a divides b, ak = b rewriting the equation $ca|cb$ as $ca|c(ak)$, which is true.

(d)the gcd of two number is the smallest linear compination of the two number so

$gcd(ka, kb)=ska+tkb$ for some integer s, t

can be rewritten as $k(sk+tb)=k\cdot gcd(a,b)$.

Problem 3.

(a) since $p|x^2-y^2$, then $p|(x+y)(x-y)$.
since $p|(x+y)(x-y)$, then $p|x+y$ or $p|x-y$, which mean $x\equiv y(mod\, p)$ and $x\equiv -y(mod\, p)$.

(b) from fermat's theorem $k^{p-1}\equiv 1(mod\, p)$, and the term $n^{\frac{p-1}{2}}$ is equal to the write side of equation iff x^2 is applied to in the equation, then $n^{p-1}\equiv 1(mod\, p)$.

(c) we can use the hint that p = 4k+3 as follows

$n^{\frac{(4k+3)-1}{2}}\equiv 1(mod\, p)$,then

$n^{2k+1}\equiv 1(mod\, p)$, multiplying both sides by n

$n^{2k+2}\equiv n(mod\, p)$, which equal

$n^{2(k+1)}\equiv n(mod\, p)$ resulting in a value of n equal to $n^{\frac{p-3}{4}+1}$.

Problem 4.

the multiples of p in the range $[0,p^k]$, is in the form of $m\cdot p$ and m can take values up to $p^{k-1}-1$,so there is exactly p^k-p^{k-1} that are relative primes to p.

Problem 5.
(a) proof by contradiction.
Suppose on turn n there exists an integer x that is not a divisor of x and y, then this contradict the game rules.

(b) proof by contradiction.
Suppose that the game ends and there exists an integer x than hasn't been written yet, then this contradicts and game rules and the game did't finish yet.

(c) if the numbers of D is the number of divisors of x and y, if this number is odd the player should go first, if it's odd the player should go second.

Problem 6.

(a) proof by contradiction
suppose that the set of primes is finite and the set is $F=\{p_1,p_2,....p_k\}$, we know that $n=p_1 p_2 ... p_k+1$,
for every $p\in F$ we know that $n\equiv 1(mod\, p)$ and since n does't have any prime factors less than it self, then n it self

is a prime, and since n is larger than the largest number in p and not in p this contradicts that the number of prime number is finite.

(b)since mod 4 divides the set of numbers into 4 sets, with remainder of 0, 1, 2, 3, for p is in the form of $p=4x+r$ and since p is odd, then r is 1 and 3.

(c)proof by contradiction
suppose that $n\equiv 3(mod\,4)$ and $p!\equiv 3(mod\,4)$, then p is either p =2 or p =1 but since n is odd, then $p\equiv 1(mod\,3)$, then $n\equiv 1(mod\,4)$ which contradict the assumption.