Max Shi

I pledge my honor that I have abided by the Stevens Honor System

CS 135 Problem Set 8

1a. $c|a \wedge c|b \Rightarrow \forall s,t \in \mathbb{Z}, c|(sa+tb)$

Because the gcd is the smallest positive linear combination of a and b, and c divides all linear combinations of a and b by the first line, then c must divide the gcd of a and b.

b. $\forall k > 0$, $\gcd(ka, kb)$ = smallest positive linear combination of ka and kb

let $s,t \in \mathbb{Z}$ and let $ska + tkb$ = smallest positive linear combination of ka and kb

$ska + tkb = k(sa+tb)$

Because $ska+tkb$ is the smallest linear combination of ka and kb, $sa+tb$ is the smallest linear combination of a and b because k is positive. Therefore, observe that we get $k(\gcd(a,b))$, which proves the statement.

c. $\gcd(a,b) = 1 \wedge \gcd(a,c) = 1$ implies that a and b do not share any factors besides 1 and a and c do not share any factors besides 1. Thus, when multiplied together, bc is the combination of the prime factorization of b and c. Therefore, a will still not share any factors with bc, and the gcd of a and bc is 1.

d. If a divides bc, this means that a shares a common factor with bc, that is not 1. Because the gcd of a and b is 1, this means a and b do not share any common factors besides 1. Therefore, dividing bc by b will not remove any of the common factors between a and bc, which means all the common factors are in c, and therefore because a and c have common factors besides 1, $a|c$.

e. Because $a \equiv \text{rem}(a,b) \bmod b$, this means that the remainder of a divided by b will maintain the same common factors that a and b share to create the gcd of a and b. Therefore, because no common factors are lost when taking the remainder of a divided by b, as therefore the gcd remains the same after the operation.

2a. $\gcd(F_8, F_6) = (21, 8) = 1$ $(F_4, F_5) = (3, 2) = 1$ $(F_7, F_6) = (13, 8) = 1$

$\gcd(F_2, F_1) = (1, 1) = 1$ $(F_5, F_4) = (5, 3) = 1$ $(F_8, F_7) = (21, 13) = 1$

$(F_3, F_2) = (2, 1) = 1$ $(F_6, F_5) = (8, 5) = 1$ $(F_9, F_8) = (34, 21) = 1$

Claim: $\gcd(F_n, F_{n-1}) = 1$

Base case: $\gcd(F_1, F_0) = \gcd(1, 0) = 1$ ✓

$\gcd(F_2, F_1) = \gcd(1, 1) = 1$ ✓

IH: $\exists k \in \mathbb{Z}$ s.t. $\gcd(F_k, F_{k-1}) = 1$ $k > 2$

Indstep: $\gcd(F_{k+1}, F_k) =$

$\gcd(F_k + F_{k-1}, F_k)$

Because $F_{k-1} \leq F_k$, for all $k > 2$, this means that $\text{rem}(F_k + F_{k-1}, F_k) = F_{k-1}$.

Thus, by GCD lemma:

$\gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, \text{rem}(F_k + F_{k-1}, F_k))$

$= \gcd(F_k, F_{k-1}) = 1$ by IH.

The claim follows by PI.

b. Let a, b, c be three consecutive Fibonacci numbers represented by F_{k+1}, F_k, and F_{k-1} respectively. By the claim proved in the last problem, $\gcd(F_{k+1}, F_k) = \gcd(F_k, F_{k-1}) = 1$.

Thus we have to prove $\gcd(F_{k+1}, F_{k-1}) = 1$.

Because $F_{k+1} = F_k + F_{k-1}$, and $F_k + F_{k-1} \equiv F_k \bmod F_{k-1}$, this means $F_{k+1} \equiv F_k \bmod F_{k-1}$. ($F_{k-1}$ is a multiple of F_{k-1})

Therefore, $\text{rem}(F_{k+1}, F_{k-1}) = \text{rem}(F_k, F_{k-1})$.

Thus, $\gcd(F_{n+1}, F_{n-1}) = \gcd(F_{n-1}, \text{rem}(F_{n+1}, F_{n-1}))$ ← by GCD Lemma
$= \gcd(F_{n-1}, \text{rem}(F_n, F_{n-1}))$
$= \gcd(F_n, F_{n-1}) \geq 1$ (started earlier in proof)
Thus, $\gcd(a, c) = 1$, and they are pairwise relatively prime

3. $\gcd(1529, 14039)$
$= \gcd(1529, 278)$
$= \gcd(278, 139)$
$= (139, 0) = 139$

$1529 \overline{)14039}$ (9) $= 13761$, remainder 278

$278 \overline{)1529}$ (5) $= 1390$, remainder 139

$139 \overline{)278}$ (2), remainder 0

$139 = 1529 - 5(278)$
$139 = 1529 - 5(14039 - 9(1529))$
$139 = 46 \cdot 1529 - 5(14039)$

Ex. a. 1, 2, 3, 4

$x \cdot 1 \equiv 1 \bmod 5$ — $x \equiv 1 \bmod 5$ — self

$x \cdot 2 \equiv 1 \bmod 5$ — $x \equiv 3 \bmod 5$ — not self. ($6 \equiv 1 \bmod 5$)

$x \cdot 3 \equiv 1 \bmod 5$ — $x \equiv 2 \bmod 5$ — not self. ($6 \equiv 1 \bmod 5$)

$x \cdot 4 \equiv 1 \bmod 5$ — $16 \equiv 1 \bmod 5$ — $x \equiv 4 \bmod 5$ — self.

1 and 4 are self-inverses.

→ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

$x \cdot 1 \equiv 1 \bmod 11$ — $1 \equiv 1 \bmod 11$ — $x \equiv 1 \bmod 11$ — self.

$x \cdot 2 \equiv 1 \bmod 11$ — $12 \equiv 1 \bmod 11$ — $x \equiv 6 \bmod 11$ — not self.

$x \cdot 3 \equiv 1 \bmod 11$ — $12 \equiv 1 \bmod 11$ — $x \equiv 4 \bmod 11$ — not self.

$x \cdot 4 \equiv 1 \bmod 11$ — $12 \equiv 1 \bmod 11$ — $x \equiv 3 \bmod 11$ — not self.

$x \cdot 5 \equiv 1 \bmod 11$ — $45 \equiv 1 \bmod 11$ — $x \equiv 9 \bmod 11$ — not self.

$x \cdot 6 \equiv 1 \bmod 11$ — $12 \equiv 1 \bmod 11$ — $x \equiv 2 \bmod 11$ — not self.

$x \cdot 7 \equiv 1 \bmod 11$ — $56 \equiv 1 \bmod 11$ — $x \equiv 8 \bmod 11$ — not self

$x \cdot 8 \equiv 1 \bmod 11$ — $56 \equiv 1 \bmod 11$ — $x \equiv 7 \bmod 11$ — not self

$x \cdot 9 \equiv 1 \pmod{11}$ $x \cdot 10 \equiv 1 \pmod{11}$

$45 \equiv 1 \pmod{11}$ $100 \equiv 1 \pmod{11}$ 9 and 10 are self-inverses.

$x \equiv 5 \pmod{11}$ $x \equiv 10 \pmod{11}$

not self. self

c k is a self-inverse if and only if $k^2 \equiv 1 \pmod{p}$.

The $\rightarrow$ direction is given in the problem, and the $\leftarrow$ direction is by definition: if $k^2 \equiv 1 \pmod{p}$, then $x \cdot k \equiv 1 \pmod{p}$ where $x \equiv k \pmod{p}$.

Also, $k^2 \equiv 1 \pmod{p}$ if and only if $k^2 - 1 \equiv 0 \pmod{p}$, by modular arithmetic lemma. Also, $k^2 - 1 \equiv 0 \pmod{p}$ if and only if $k^2 - 1$ is a multiple of p. Because $k^2 - 1 = (k-1)(k+1)$, one of these factors must be p. Because $k < p$, we can only choose $k = p-1$ so that $(p-1+1) = p$. $p+1$ is impossible the only other number that satisfies this is $k = 0$, because 0 is a multiple of any number. Thus, 0 and $p-1$ are the only numbers that satisfy this premise

∎