Anooj Pai HW3

1) is $4^{1536} \equiv 9^{4824} \bmod 35$

$35 = 5 \cdot 7$, we know 5 and 7 are primes.
If we use Fermat's little theorem, any prime p that $1 \leq a \leq p$, we find that $a^{p-1} \equiv 1 \bmod p$.
If we plug in 5 and 7 we get $a^{5-1} \equiv 1 \bmod 5$ and $a^{7-1} \equiv 1 \bmod 7$. Then $(a^{5-1})^{7-1} = a^{24} \equiv 1 \bmod 35$.
This means $a^{24} \equiv 1 \bmod 35$ for $1 \leq a \leq 35$. If we divide 1536 and 4824 by 24, we get 64 and 201 respectively. So $4^{1536} = 4^{24 \cdot 64} \equiv 1 \bmod 35$ and $9^{4824} = 9^{24 \cdot 201} \equiv 1 \bmod 35$. Because they both are equivalent we have proven $4^{1536} \equiv 9^{4824} \bmod 35$.

2) solve $x^{86} \equiv 6 \bmod 29$

we know that 6 is relatively prime to 29, this means that x would be the same.
By using Fermat's little theorem we find that the equation can be written as $x^{28} \equiv 1 \bmod 29$.
When we rewrite the equation we get,
$x^{86} \equiv x^2 \bmod 29 \rightarrow x^2 \equiv 6 \bmod 29 \rightarrow x^2 \equiv 64 \bmod 29$.
if we factor $x^2 - 64$ we get $(x+8)(x-8) = 0 \bmod 29$
By this we have found that 8 and 29 are the

solutions for $x^{60} \equiv 6 \bmod 29$.

3) <u>Prove $\gcd(f_{n+1}, f_n) = 1$ for $n \geq 1$</u>

Prove that 2 consecutive Fib nums are relatively prime:

say $ax + by = \gcd(a,b)$ and $\gcd(a+b, b)$

then $(a+b)x + by = \gcd(a+b, b)$

now $ax + bm = \gcd(a,b)$

if we let $m = x+y$ then $ax + bm = \gcd(a,b)$

becomes $ax + b\,x{+}y = \gcd(a,b)$

then $ax + bx + by = \gcd(a,b)$

or

$(a+b)x + by = \gcd(a,b)$

now we see that $\gcd(a+b, b) = \gcd(a,b)$

From this we see that $\gcd(f_{n+1}, f_n) = 1$

This proves that 2 consecutive Fib numbers are relatively prime.