# Exercises 3: second batch solutions 5, 6, 7, 8

5. $5^4 \cdot 2^{28} + 2^{32} = (5^4 + 2^4) \cdot 2^{28} \therefore 641 \mid 5^4 \cdot 2^{28} + 2^{32}$.

$$5^4 \cdot 2^{28} - 1 = (5 \cdot 2^7)^4 - 1$$
$$= ((5 \cdot 2^7)^2 - 1)((5 \cdot 2^7)^2 + 1)$$
$$= (5 \cdot 2^7 - 1)(5 \cdot 2^7 + 1)((5 \cdot 2^7)^2 + 1)$$

$\therefore 641 \mid 5^4 \cdot 2^{28} - 1$

But $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 5^4 \cdot 2^{28} + 2^{32} - (5^4 \cdot 2^{28} - 1)$

$\therefore 641 \mid F_5$. It follows that $F_5$ is not a prime.

6. I've stolen this proof from one of the class because I like it more than mine. We observe the pattern

$$a^2 - 1 = (a+1)(a-1)$$
$$a^4 - 1 = (a^2)^2 - 1 = (a^2+1)(a^2-1) = (a^2+1)(a+1)(a-1)$$
$$a^8 - 1 = (a^4+1)(a^2+1)(a+1)(a-1)$$
$$a^{16} - 1 = (a^8+1)(a^4+1)(a^2+1)(a+1)(a-1)$$

prove this in general

It follows that $F_n - 2 = 2^{2^n} - 1$ will have as a factor

$2^{2^m} + 1$ since $m < n$.

I like this proof because you can see clearly why the result is true.

7. Suppose that there are only finitely many primes of the form $4q+3$. Let these be $p_1, \dots, p_k$. Put $N = 4p_1 \dots p_k - 1$.

Observe that $N$ is odd. It follows that any primes that divide it must be odd and so either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$.

Not all prime factors can be $\equiv 1 \pmod 4$ because the product of any nos $\equiv 1 \pmod 4$ is again a no. $\equiv 1 \pmod 4$. And $N \equiv 3 \pmod 4$.

It follows that $N$ must be divisible by a prime $\equiv 3 \pmod 4$ but this contradicts our original assumption that there are only finitely many such primes.

8.

| $f_0$ | $f_1$ | $f_2$ | $f_3$ ... |
|---|---|---|---|
| 0 | 1 | 1 | 2 ... |

Base case when $n=1$, $f_0 = 0$, $f_1 = 1$, $f_2 = 1$ also we get the matrix on the RHS.

IH Assume $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$.

Proof plan we calculate $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1}$:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} f_{n+1} + f_n & f_n + f_{n-1} \\ f_{n+1} & f_n \end{pmatrix} = \begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix} \checkmark$$

$$\det \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \left(\det \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right)^n = (-1)^n$$

$$\det \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = f_{n+1} f_{n-1} - f_n^2$$

$$\therefore \quad (-1)^n = f_{n+1} f_{n-1} - f_n^2$$

n even

$$1 = f_{n+1} f_{n-1} - f_n^2 \qquad (1)$$

n odd

$$1 = f_n^2 - f_{n+1} f_{n-1} \qquad (2)$$

The results imply $\gcd(f_n, f_{n+1}) = 1$ & (1) & (2) are Bézout's Identity applied to consecutive Fibonacci #'s.