# Math 312: Lecture 5

John Roe

Penn State University

January 24, 2014

# Response to quiz

Homework 1 (late due date, 20 percent penalty) is due today. Remember, homework must be *stapled with a cover-sheet*.

# Mathematical Induction

Mathematical induction is a special technique for proving a "for all statement"

$$\forall n \in \mathbb{N}\ P(n)$$

where the quantification is over the *natural numbers* ($\mathbb{N} = \{1, 2, 3, \ldots\}$.) It says that if we can prove

- $P(1)$ (the "base case"), and
- $\forall k \in \mathbb{N}\ (P(k) \Rightarrow P(k+1))$ (the "induction step")

then $\forall n \in \mathbb{N}\ P(n)$ will follow.

Think of the various propositions $P(1)$, $P(2)$, $P(3)$ and so on as being like a row of dominoes.

If we can knock over the first domino (the base case, $P(1)$)... and if each domino knocks over the next one (the induction step, $P(k) \Rightarrow P(k+1)$)... then all the dominoes must fall ($\forall n \in N \; P(n)$).

# Formal statement

| Kind of Statement | Strategies to Transform (when statement is a *goal*) | Strategies to Infer (when statement is a *given*) |
|---|---|---|
| Universal statement for all natural numbers, $\forall n \in \mathbb{N}\ P(n)$ | **Proof by induction:** Prove $P(1)$ and also prove $\forall n \in \mathbb{N}\ P(n) \Rightarrow P(n+1)$ | |

# An example: Fermat numbers

**Definition**

The *Fermat number* $F_n = 2^{2^n} + 1$.

| $n$ | $2^n$ | $F_n = 2^{2^n} + 1$ |
|---|---|---|
| 0 | 1 | 3 |
| 1 | 2 | 5 |
| 2 | 4 | 17 |
| 3 | 8 | 257 |
| 4 | 16 | 65537 |

Notice $F_0 F_1 = 3 \times 5 = 15 = F_2 - 2$,
$F_0 F_1 F_2 = 3 \times 5 \times 17 = 255 = F_3 - 2$,
$F_0 F_1 F_2 F_3 = 3 \times 5 \times 17 \times 257 = 65535 = F_4 - 2$. Will this pattern continue?

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

5: **Induction step:** We must show that **if** $F_0 \cdots F_k = F_{k+1} - 2$, **then** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

6: **Suppose that** $F_0 \cdots F_k = F_{k+1} - 2$

11: **Thus** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$. **We conclude that** $F_0 \cdots F_k = F_{k+1} - 2$ **implies** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

5: **Induction step:** We must show that **if** $F_0 \cdots F_k = F_{k+1} - 2$, **then** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

6: **Suppose that** $F_0 \cdots F_k = F_{k+1} - 2$

7: By the inductive hypothesis and the definition of Fermat numbers, $F_0 \cdots F_k = 2^{2^{k+1}} - 1$.

11: **Thus** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$. **We conclude that** $F_0 \cdots F_k = F_{k+1} - 2$ **implies** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

5: **Induction step:** We must show that **if** $F_0 \cdots F_k = F_{k+1} - 2$, **then** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

6: **Suppose that** $F_0 \cdots F_k = F_{k+1} - 2$

7: By the inductive hypothesis and the definition of Fermat numbers, $F_0 \cdots F_k = 2^{2^{k+1}} - 1$.

8: Then $F_0 \cdots F_{k+1} = (F_0 \cdots F_k) \cdot F_{k+1} =$

11: **Thus** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$. **We conclude that** $F_0 \cdots F_k = F_{k+1} - 2$ **implies** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

5: **Induction step:** We must show that **if** $F_0 \cdots F_k = F_{k+1} - 2$, **then** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

6: **Suppose that** $F_0 \cdots F_k = F_{k+1} - 2$

7: By the inductive hypothesis and the definition of Fermat numbers, $F_0 \cdots F_k = 2^{2^{k+1}} - 1$.

8: Then $F_0 \cdots F_{k+1} = (F_0 \cdots F_k) \cdot F_{k+1} =$

9: $= (2^{2^{k+1}} - 1)(2^{2^{k+1}} + 1) = \left(2^{2^{k+1}}\right)^2 - 1 =$

11: **Thus** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$. **We conclude that** $F_0 \cdots F_k = F_{k+1} - 2$ **implies** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

1: **Theorem:** For all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$

2: **We will prove by induction** that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

3: **Base case:** We must prove $F_0 \cdots F_1 = F_{1+1} - 2$

4: This is clear: $3 \times 5 = 15 = 17 - 2$.

5: **Induction step:** We must show that **if** $F_0 \cdots F_k = F_{k+1} - 2$, **then** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

6: **Suppose that** $F_0 \cdots F_k = F_{k+1} - 2$

7: By the inductive hypothesis and the definition of Fermat numbers, $F_0 \cdots F_k = 2^{2^{k+1}} - 1$.

8: Then $F_0 \cdots F_{k+1} = (F_0 \cdots F_k) \cdot F_{k+1} =$

9: $= (2^{2^{k+1}} - 1)(2^{2^{k+1}} + 1) = \left(2^{2^{k+1}}\right)^2 - 1 =$

10: $= 2^{2^{k+2}} - 1 = F_{k+2} - 2$.

11: **Thus** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$. **We conclude that** $F_0 \cdots F_k = F_{k+1} - 2$ **implies** $F_0 \cdots F_{(k+1)} = F_{(k+1)+1} - 2$

12: **By mathematical induction**, this completes the proof that $F_0 \cdots F_n = F_{n+1} - 2$ for all natural numbers $n \geqslant 1$

13: Thus we have shown for all natural numbers $n$, $F_0 F_1 \cdots F_n = F_{n+1} - 2$, as required. $\square$

# Primes and Fermat numbers

Fermat guessed that all the $F_n$ were prime. $F_0$ through $F_4$ are indeed prime, but

$$F_5 = 4294967297 = 6700417 \times 641.$$

However, one does have

**Theorem**

*No two different Fermat numbers have a prime factor in common.*

Since there are infinitely many Fermat numbers, and each has at least one prime factor that doesn't belong to any of the others, this shows that there are infinitely many primes.

1: **Theorem:** No two Fermat numbers have a common prime factor

9: Thus we have shown no two Fermat numbers have a common prime factor, as required. $\square$

1: **Theorem:** No two Fermat numbers have a common prime factor

2: **Assume, seeking a contradiction** that the statement "no two Fermat numbers have a common prime factor" is **false**.

8: **This contradiction shows that our assumption was false** and thus that no two Fermat numbers have a common prime factor.

9: Thus we have shown no two Fermat numbers have a common prime factor, as required. □

1: **Theorem:** No two Fermat numbers have a common prime factor

2: **Assume, seeking a contradiction** that the statement "no two Fermat numbers have a common prime factor" is **false**.

3: Then there is a prime $p$ that divides both $F_m$ and $F_{m+k}$, for some natural numbers $m, k$.

4: Notice that $p$ must be odd, since all the Fermat numbers are odd.

8: **This contradiction shows that our assumption was false** and thus that no two Fermat numbers have a common prime factor.

9: Thus we have shown no two Fermat numbers have a common prime factor, as required. $\square$

1: **Theorem:** No two Fermat numbers have a common prime factor

2: **Assume, seeking a contradiction** that the statement "no two Fermat numbers have a common prime factor" is **false**.

3: Then there is a prime $p$ that divides both $F_m$ and $F_{m+k}$, for some natural numbers $m, k$.

4: Notice that $p$ must be odd, since all the Fermat numbers are odd.

5: Since $p$ divides $F_m$, it also divides the product $F_1 \cdots F_{m+k-1}$, which equals $F_{m+k} - 2$ by our previous theorem.

8: **This contradiction shows that our assumption was false** and thus that no two Fermat numbers have a common prime factor.

9: Thus we have shown no two Fermat numbers have a common prime factor, as required. $\square$

1: **Theorem:** No two Fermat numbers have a common prime factor

2: **Assume, seeking a contradiction** that the statement "no two Fermat numbers have a common prime factor" is **false**.

3: Then there is a prime $p$ that divides both $F_m$ and $F_{m+k}$, for some natural numbers $m$, $k$.

4: Notice that $p$ must be odd, since all the Fermat numbers are odd.

5: Since $p$ divides $F_m$, it also divides the product $F_1 \cdots F_{m+k-1}$, which equals $F_{m+k} - 2$ by our previous theorem.

6: Since $p$ divides $F_{m+k}$ and $F_{m+k} - 2$, it divides 2.

7: But this is a contradiction: no odd prime divides 2.

8: **This contradiction shows that our assumption was false** and thus that no two Fermat numbers have a common prime factor.

9: Thus we have shown no two Fermat numbers have a common prime factor, as required. $\square$