Reminders

- PS B Draft due tomorrow
- PS A Final due Friday
- PS C Draft due Monday

Quick Summary

① Induction

If we want to prove some collection of statements $S(n)$, one for each integer $n \geq 1$, induction gives us a strategy for doing this:

- First prove $S(1)$ is true. (Base case)
- Then prove that, if $S(k)$ is true for some k, then $S(k+1)$ is also true. (ie, $S(k) \Rightarrow S(k+1)$). (Inductive step)

We know $S(1)$ is true. Our inductive step $S(1) \Rightarrow S(2)$, and since $S(1)$ is true, we must have $S(2)$ true also. Again by our inductive step, $S(2) \Rightarrow S(3)$, and since $S(2)$ is true, $S(3)$ must be too! And so on.

Variant: Base case is different ($n=0$, or $n=8$, ...), Strong induction

② Euclid's lemma

- If p is prime and $p \mid ab$ for some $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.
- If p is prime and $p \mid a_1 \cdots a_n$ for $a_1, \ldots, a_n \in \mathbb{Z}$, then $p \mid a_i$ for some $i = 1, \ldots, n$.

Statement is not true if p is not prime:

$p=10$ $a=2$ $b=5$ $10 \mid 2 \cdot 5$ but $10 \nmid 2$ and $10 \nmid 5$.

③ Fundamental Thm of Arithmetic

Any integer $n \geq 2$ can be written uniquely in the form $n = p_1^{e_1} \cdots p_r^{e_r}$ for distinct primes $p_1, \ldots, p_r$ and positive integers $e_1, \ldots, e_r$.

$$21 = 3^1 \cdot 7^1$$
$$12 = 2^2 \cdot 3^1$$

Worksheet 7

① Want to show that $\frac{(2n)!}{2^n \cdot n!}$ is an integer for all $n \geq 0$.

We'll induct on n. Our base case is n=0, and

$$\frac{(2\cdot 0)!}{2^0 \cdot 0!} = \frac{1}{1\cdot 1} = 1 \in \mathbb{Z}.$$

Next, we have the inductive step. For this, we assume that $\frac{(2k)!}{2^k \cdot k!} \in \mathbb{Z}$ for some k and we want to show that $\frac{(2(k+1))!}{2^{k+1}(k+1)!} \in \mathbb{Z}$.

(Jingyi)

$$\frac{(2(k+1))!}{2^{k+1}(k+1)!} = \frac{(2k+2)!}{2^{k+1}(k+1)!} = \frac{(2k+2)(2k+1)(2k)!}{2^{k+1}(k+1)!}$$

$$= \frac{(2k+2)(2k+1)(2k)!}{2^k \cdot 2\ (k+1)\cdot k!}$$

$$= \frac{(2k+2)(2k+1)}{2\cdot(k+1)} \cdot \frac{(2k)!}{2^k \cdot k!}$$

$$= (2k+1)\cdot \frac{(2k)!}{2^k \cdot k!}$$

Since $2k+1$ is an integer and $\frac{(2k)!}{2^k \cdot k!}$ is an integer, the product is also an integer, so this completes the induction. □

② want to show that $15 \mid 2^{4n}-1$ for all non-negative n. (includes n=0)

We'll induct on n. Our base case is n=0, and we check that

$$2^{4\cdot 0}-1 = 1-1 = 0$$

is divisible by 15. For inductive step, we assume $15 \mid 2^{4k}-1$ for some k, and we want to show that $15 \mid 2^{4(k+1)}-1$.

$$2^{4(k+1)} = 15a+1.$$
$$2^{4k}\cdot 2^4 - 1 = 15a$$
$$2^{4k}\cdot 16 - 1 = 15a$$

(we)

$2^{4(k+1)}-1 = 2^{4k+4}-1 = 2^{4k}\cdot 16 - 1$. Since $15 \mid 2^{4k}-1$, I know there exists some a such that $2^{4k}-1 = 15a$. So $2^{4k} = 15a+1$. So

$$2^{4k}\cdot 16 - 1 = (15a+1)\cdot 16 - 1$$
$$= 15\cdot 16a + 16 - 1$$
$$= 15\cdot 16a + 15$$
$$= 15(16a+1)$$

so $15 \mid 2^{4(k+1)}-1$. □

(Ellie)

Different approach: know $2^{4k}-1 = 15a$ for some a.

$$(2^{4k}-1)\cdot 2^4 = 2^4 \cdot 15a$$
$$2^{4(k+1)} - 2^4 = 2^4 \cdot 15a$$
$$2^{4(k+1)} - 2^4 + 2^4 - 1 = 2^4 \cdot 15a + 2^4 - 1$$
$$2^{4(k+1)} - 1 = 2^4 \cdot 15a + 15$$
$$= 15(2^4 a + 1)$$

so again $2^{4(k+1)}-1$ is divisible by 15. □

③ $F_1 = F_2 = 1$. $F_n = F_{n-1} + F_{n-2}$.

want to show that F_n is even if and only if $3 \mid n$.

We have $S(n) =$ "F_n is even if and only if $3 \mid n$"

sometimes, it can help to write down very clearly what statement it is that you're trying to prove by induction.

We'll want to prove this by (strong) induction.

For $n=1$, we want to show that $S(1)$ is true, ie, that "F_1 is even iff $3 \mid 1$"

we know that $F_1 = 1$ is odd and we know that $3 \nmid 1$. so $S(1)$ is a biconditional of the form $F \Leftrightarrow F$, which is true!

For $n=2$, we want to show that $S(2)$ is true, ie, that "F_2 is even iff $3 \mid 2$", but this is also a true statement for the same reasons.

Next we have the inductive step. This has to be strong induction, so we assume that $S(1), S(2), \ldots, S(k)$ are all true. We want to show that $S(k+1)$ is true.

In particular, we know that $S(k-1)$ & $S(k)$ are both true.

$$F_{k+1} = F_k + F_{k-1}$$

Case 1 Say $k+1 \equiv 0 \pmod 3$. Then $k \equiv -1 \equiv 2 \pmod 3$ and $k-1 \equiv -2 \equiv 1 \pmod 3$, so $3 \nmid k$ and $3 \nmid k-1$, so, since $S(k)$ & $S(k-1)$ are true, it must be that F_k & F_{k-1} are both odd. But then F_{k+1} is a sum of two odds, so its even, so $S(k+1)$ is true. (Recall $S(k+1)$ says "F_{k+1} is even $\Leftrightarrow 3 \mid k+1$" and we have both F_{k+1} even & $3 \mid k+1$ in this case.)

Case 2 Say $k+1 \equiv 1 \pmod 3$. Then $k \equiv 0 \pmod 3$, so F_k is even. Also, $k-1 \equiv -1 \equiv 2 \pmod 3$ so F_{k-1} is odd. So F_{k+1} is the sum of an even & an odd, so its odd, so $S(k+1)$ is true.

Case 3 Say $k+1 \equiv 2 \pmod 3$. Then $k \equiv 1 \pmod 3$, so F_k is odd, and $k-1 \equiv 0 \pmod 3$, so F_{k-1} is even, so F_{k+1} is the sum of an odd & an even, so its odd, so $S(k+1)$ is true.

This completes our induction. □

④ If $p_1, \dots p_n$ are distinct primes, want to show that $\sqrt{p_1 \cdots p_n}$ is irrational.

(*)

- Prove that $\sqrt{p_1}$ is irrational. Suppose $\sqrt{p_1} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $\gcd(a,b)=1$. Then $p_1 b^2 = a^2$. Then $p_1 | a^2$, so by Euclid's lemma, we know that $p | a$.

(Porter)

so $a = p_1 x$ for some $x \in \mathbb{Z}$.

$$p_1 b^2 = a^2 = (p_1 x)^2 = p_1^2 x^2$$
$$b^2 = p_1 x^2$$

so $p_1 | b^2$, so by Euclid's lemma, $p_1 | b$. so p_1 is a common factor of a & b, contradicting $\gcd(a,b)=1$.

- We're trying to prove by induction that

$S(n) =$ "$\sqrt{p_1 \cdots p_n}$ is prime for n distinct primes $p_1, \dots, p_n$"

and we're just shown that $S(1)$ is true.

Assume $S(k)$ is true and we want to prove $S(k+1)$. so suppose $p_1, \dots, p_k, p_{k+1}$ are $k+1$ distinct primes.

$$\sqrt{p_1 \cdots p_k p_{k+1}} = \sqrt{p_1}\sqrt{p_2 \cdots p_k}.$$

from base case, this is irrational

from $S(k)$, this is irrational.

but the product of two irrationals can be rational!

eg, $\sqrt{2} \cdot \sqrt{2} = 2$.

Let's just use our strategy in (*) to prove this in general directly & without induction!

Suppose for a contradiction that $\sqrt{p_1 \cdots p_n} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $\gcd(a,b)=1$. Rearranging, $p_1 \cdots p_n b^2 = a^2$. Then $p_1 | a^2$, so by Euclid's lemma, $p | a$. so there exists an x such that $a = p_1 x$.

$$p_1 \cdots p_n b^2 = a^2 = (p_1 x)^2 = p_1^2 x^2$$
$$p_2 \cdots p_n b^2 = p_1 x^2$$

$p_1 | p_2 \cdots p_n b^2$. But p_1 cannot divide $p_2, \dots, p_n$ since all of those are primes that are distinct from p_1. so Euclid's lemma tells us that $p_1 | b^2$, so $p_1 | b$.

So p_1 is a common factor of a & b, contradicting $\gcd(a,b)=1$. □

⑤ $p_1, p_2, \ldots$ in ascending order. Want to show that $p_n \le p_1 \cdots p_{n-1} - 1$ for all $n \ge 3$.

Let $a = p_1 \cdots p_{n-1} - 1$. Since $p_1 = 2$ & $p_2 = 3$, $a \ge 2 \cdot 3 - 1 = 5 \ge 2$, so by the fundamental thm of arithmetic, a has some prime factor q.

Notice that $a \equiv 0 \pmod{q}$ but $a \equiv -1 \pmod{p_i}$ for all $i = 1, \ldots, n-1$.

So $q \neq p_1, \ldots, p_{n-1}$. But $p_1, p_2, \ldots$ is a list of primes in increasing order, so $q \ge p_n$. But then

$$p_n \le q \le a = p_1 \cdots p_{n-1} - 1.$$ □

$$\begin{aligned} a &= p_1 \cdots p_{i-1} p_i p_{i+1} \cdots p_{n-1} - 1 \\ &\equiv p_1 \cdots p_{i-1} \cdot 0 \cdot p_{i+1} \cdots p_{n-1} - 1 \pmod{p_i} \\ &= 0 - 1 \pmod{p_i} \\ &= -1 \pmod{p_i} \end{aligned}$$

since $p_i \equiv 0 \pmod{p_i}$, can swap out p_i for 0 in big product!

⑥ $1100 = 11 \cdot 100 = 11 \cdot 4 \cdot 25 = 11^1 2^2 5^2$

$p_1 = 11$ $e_1 = 1$
$p_2 = 2$ $e_2 = 2$
$p_3 = 5$ $e_3 = 2$

$n = 3$ = # of prime factors.

$a \ge 2$ is an integer. By fundamental thm, there exist distinct primes $p_1, \ldots, p_n$ and positive integers such that $a = p_1^{e_1} \cdots p_n^{e_n}$. Want to show a is a perfect square iff e_i is even for all i.

(Mustafa)

ⓐ If a is a perfect square, then $\sqrt{a} = b$ for some integer b. Then b must have exactly the same set of prime factors as a, so by the fundamental thm, we can write $b = p_1^{f_1} \cdots p_n^{f_n}$ for some positive integers $f_1, \ldots, f_n$. Then

$$\begin{aligned} a &= b^2 \\ p_1^{e_1} \cdots p_n^{e_n} &= \left(p_1^{f_1} \cdots p_1^{f_n}\right)^2 \\ &= p_1^{2f_1} \cdots p_1^{2f_n} \end{aligned}$$

Since prime factorizations are unique, we must have $e_i = 2f_i$ for all i, so e_i is even.

Conversely, if e_i is even for all i, we can write $e_i = 2f_i$ for some integer f_i. and then

$$\sqrt{a} = \sqrt{p_1^{e_1} \cdots p_n^{e_n}} = \sqrt{p_1^{2f_1} \cdots p_n^{2f_n}} = p_1^{f_1} \cdots p_n^{f_n} \in \mathbb{Z}$$

so a is a perfect square. □

(b) By division algorithm, we can write $e_i = 2f_i + r_i$ for $r_i \in \{0,1\}$, and e_i is even if and only if $r_i = 0$ for all i.

a is a perfect square if and only if $\sqrt{a}$ is an integer.

So we want to show that $\sqrt{a}$ is an integer iff $r_i = 0$ for all i.

(Singyi)

Notice that

$$\sqrt{a} = \sqrt{p_1^{e_1} \cdots p_n^{e_n}} = \sqrt{p_1^{2f_1+r_1} \cdots p_n^{2f_n+r_n}}$$

$$= \sqrt{p_1^{2f_1} \cdots p_n^{2f_n} p^{r_1} \cdots p_n^{r_n}}$$

$$= p_1^{f_1} \cdots p_n^{f_n} \sqrt{p_1^{r_1} \cdots p_n^{r_n}}$$

If $r_i = 0$ for all i, then the stuff under square root is 1, so $\sqrt{a}$ is an integer.

If there exists an i such that $r_i \neq 0$, then the stuff under the square root is a product of distinct primes, so by #4, it's irrational. So $\sqrt{a}$ is also irrational, so it's not an integer. □