$-9 \equiv ?$ $\pmod{11}$

≥ 0

< 11

$-9 : (\quad) \cdot 11 +$ ( )

$15237 \equiv ?$ $\pmod{15237}$

0

$1900005 \equiv ?$ $\pmod{10}$

7

1900000

$-9 \equiv -9 \equiv -20 \equiv 2 \pmod{11}$

$42156392745 \equiv 0 \pmod{3}$

$10 \equiv 1 \pmod{13}$

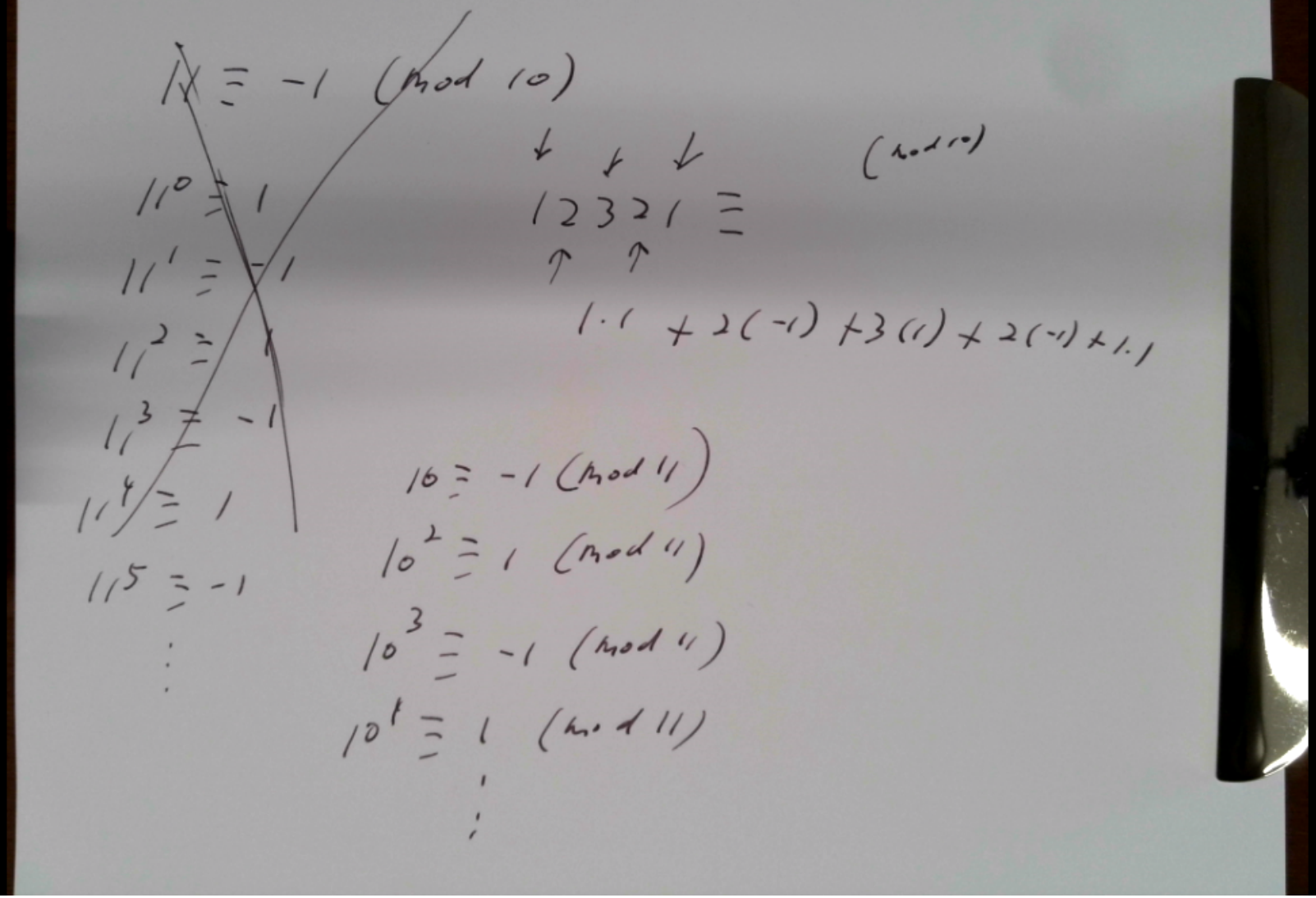
$14136 \equiv 6 + 3 \cdot 10 + 1 \cdot 10^2 + 4 \cdot 10^3 + 1 \cdot 10^4$

$\pmod{3}$

$\equiv 6 + 3 \cdot 1 + 1 \cdot 1^2 + 4 \cdot 1^3 + 1 \cdot 1^4$

$\equiv 6 + 3 + 1 + 4 + 1$

$10 \equiv 1 \pmod{9}$


11 ≡ -1 (mod 10)
11^0 ≡ 1
11^1 ≡ -1
11^2 ≡ 1
11^3 ≡ -1
11^4 ≡ 1
11^5 ≡ -1
10 ≡ -1 (mod 11)
10^2 ≡ 1 (mod 11)
10^3 ≡ -1 (mod 11)
10^4 ≡ 1 (mod 11)
(mod 10)
12321 ≡
1·1 + 2(-1) + 3(1) + 2(-1) + 1·1

GCD(27, 3)

$27 = 9 \cdot 3 + 0$

5) Find $2^{130} \pmod 7$ using modular exp.

$2^1 \equiv 2$

$2^2 = (2^1)^2 \equiv 2^2 \equiv 4$

$2^4 = (2^2)^2 \equiv 4^2 \equiv 16 \equiv 2$

$2^8 \equiv 2^2 \equiv 4$

$2^{16} \equiv 2$

$2^{32} \equiv 4$

$2^{64} \equiv 2$

$2^{128} \equiv 4$

$130 = 128 + 2$

$2^{130} = 2^{(128+2)}$

$= 2^{128} \cdot 2^2$

$\equiv 4 \cdot 4$

$\equiv 16 \equiv 2$

find $2^{6002} \pmod 7$ using FLT

By FLT, $2^6 \equiv 1 \pmod 7$

$2^{6000} \equiv (2^6)^{1000} \equiv 1^{1000} \equiv 1$

$2^{6001} \equiv 1 \cdot 2 \equiv 2$

$2^{6002} \equiv 2 \cdot 2 \equiv \boxed{4}$

Induction

Suppose you wish to prove that a family of propositions $P(n)$ $(n \in \mathbb{Z},\ n \geq 0)$ is always true (i.e. prove $P(0), P(1), P(2), P(3), \ldots$ are all true).

It suffices to prove just 2 things:

(1) $P(0)$

(2) $P(n) \rightarrow P(n+1)$ $\quad (n \geq 0)$

If you can prove (1) & (2), then you can say

$P(n)$ is true for <u>all</u> $n \geq 0$.

Reason: "Mathematical Induction"

Example

Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $n \geq 1$

~~Proof:~~ Let $P(n)$ be the proposition $1+2+\dots+n = \frac{n(n+1)}{2}$

Prove $P(n)$ $\forall n \geq 1$

I. Base case: Prove $P(1)$ is true

$P(1)$ says $1 = \frac{1(1+1)}{2}$ This is true ✓

II. Inductive Step

Prove $P(n) \rightarrow P(n+1)$ $(n \geq 1)$

$P(n)$ is the prop: $1+2+\cdots+(n-2)+(n-1)+n = \frac{n(n+1)}{2}$

Prove $P(n) \rightarrow P(n+1)$

1. $P(n)$ Hypothesis

2. $1+2+\cdots+(n-1)+n = \frac{n(n+1)}{2}$ Def. of $P(n)$

3. $\left[1+2+\cdots+(n-1)+n\right]+(n+1) = \left[\frac{n(n+1)}{2}\right]+(n+1)$ Subs. (2)

$= \frac{n^2+n}{2} + \frac{2(n+1)}{2} = \frac{n^2+n+2n+2}{2} = \frac{(n+1)(n+2)}{2}$ algebra

4. $P(n+1)$ 3 def of $P(n+1)$

$\therefore P(n) \rightarrow P(n+1)$

$\therefore P(n)\ \forall n \geq 1$ Math. Ind.

QED

Prove $1+3+\cdots+(2n-1) = n^2$

Let $P(n)$ be the prop $1+3+\cdots+(2n-1)=n^2 \quad (n \geq 1)$

Prove $P(n)$ $\forall n \geq 1$

Proof:

I. Base case: prove $P(1)$. $P(1)$ says $1=1^2$ (true) ✓

II. prove $P(n) \Rightarrow P(n+1) \quad (n \geq 1)$

1. $P(n)$ Hyp.
2. $1+3+\cdots+(2n-1)=n^2$ Def of $P(n)$
3. $\underbrace{1+3+\cdots+(2n-1)}+(2n+1) = n^2+(2n+1)$ alg (add $2n+1$)

$= \cancel{n^2+2n+1}$ $= (n+1)^2$ alg

4. $P(n+1)$ 3. def of $P(n+1)$

$\therefore P(n) \Rightarrow P(n+1) \quad (n \geq 1)$

$\therefore P(n)$ $\forall n \geq 1$

QED

Prove $1+2+4+\cdots+2^n = 2^{n+1}-1$ $\quad n \geq 0$

Let $P(n)$ be the prop $1+2+\cdots+2^n = 2^{n+1}-1$

Prove $P(n)$ $\forall n \geq 0$

Base case: $P(0)$ says $1 = 2^1 - 1$ (true)

Prove $P(n) \rightarrow P(n+1)$ $\quad n \geq 0$

1. $P(n)$ Hyp.
2. $1+2+4+\cdots+2^n = 2^{n+1}-1$ Def of $P(n)$
3. $(1+2+4+\cdots+2^n)+2^{n+1} = 2^{n+1}-1+2^{n+1}$ Add 2^{n+1} to both sides of prop 2

$= 2(2^{n+1}) - 1$

$= 2^{n+2} - 1$

4. $P(n+1)$ Def of $P(n+1)$, 3.

$\therefore P(n) \rightarrow P(n+1)$

$\therefore P(n)$ $\forall n \geq 0$

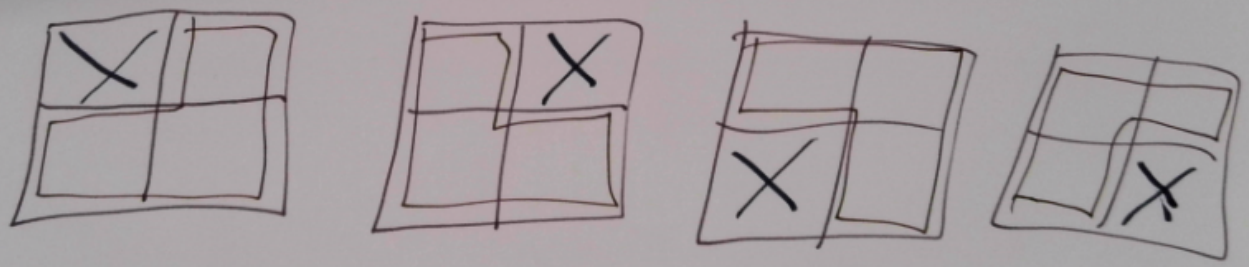
QED

Prove: you can tile a $2^n \times 2^n$ room with one missing square using L-shaped tiles.

Let $P(n)$ be the prop: you can tile a $2^n \times 2^n$ room w/ one missing square using L-shaped tiles.

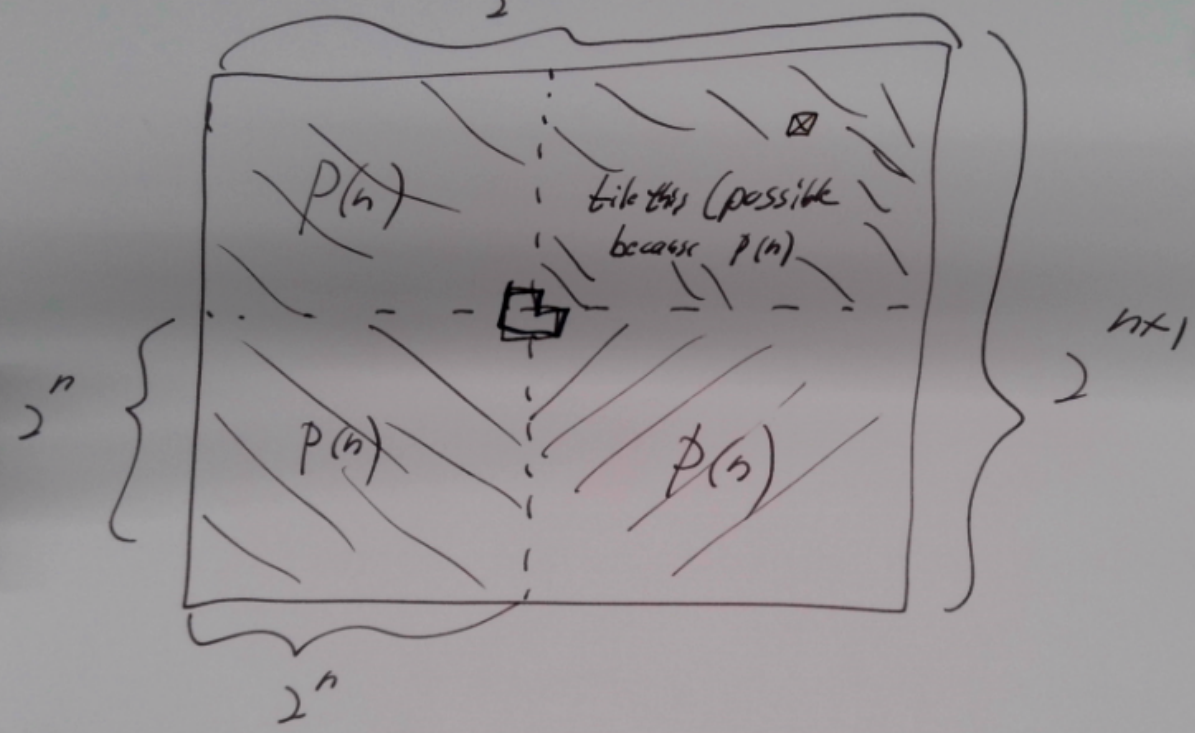
Prove $P(n)$ $\forall n \geq 1$

Base Case: $P(1)$ says you can tile a 2×2 room



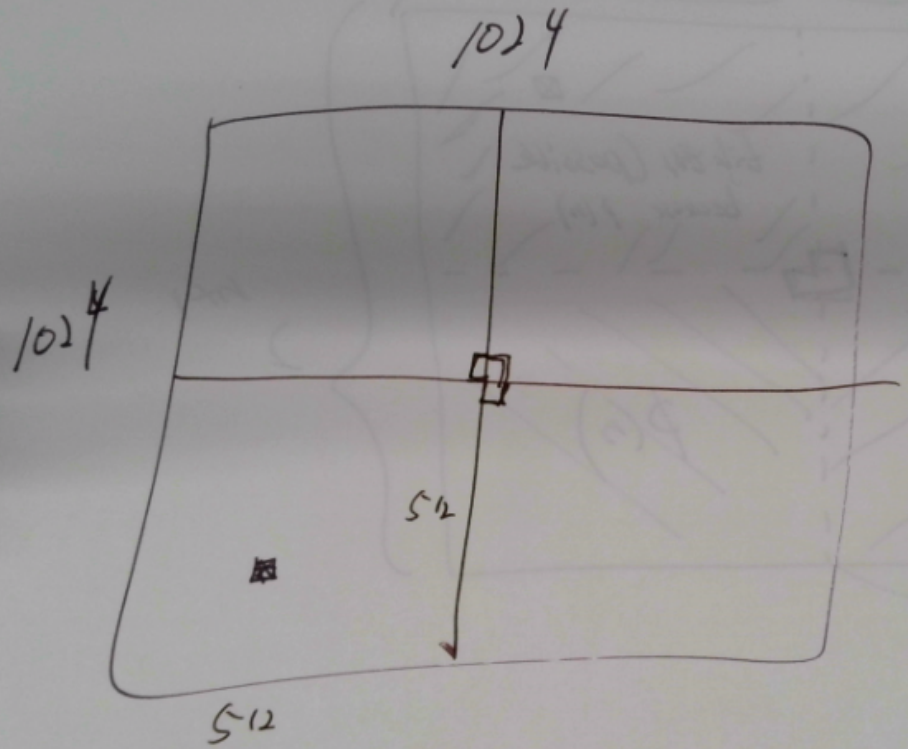
$\therefore P(1)$ is true

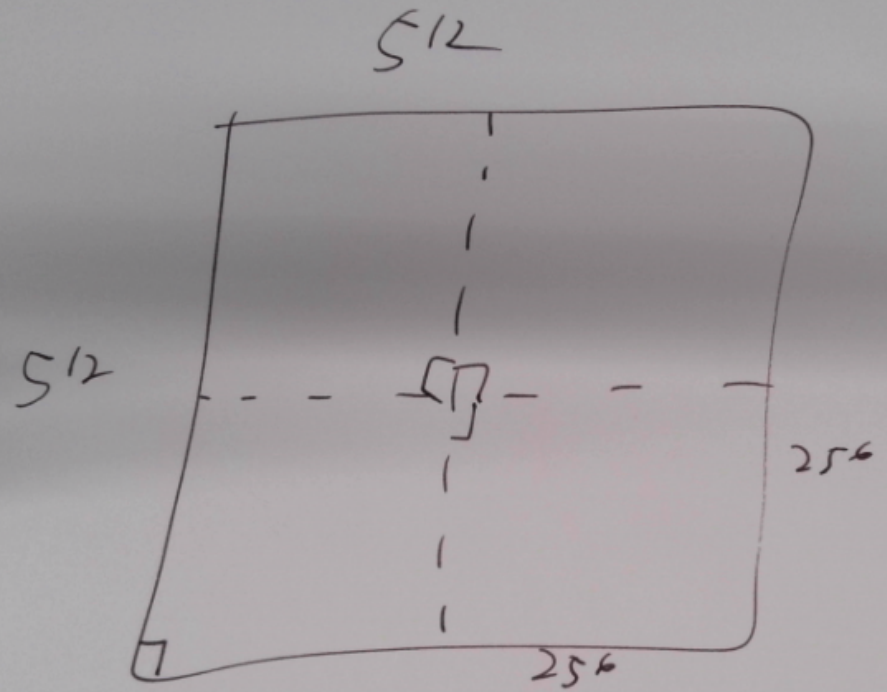
Prove $P(n) \rightarrow P(n+1)$ $\quad n \geq 1$

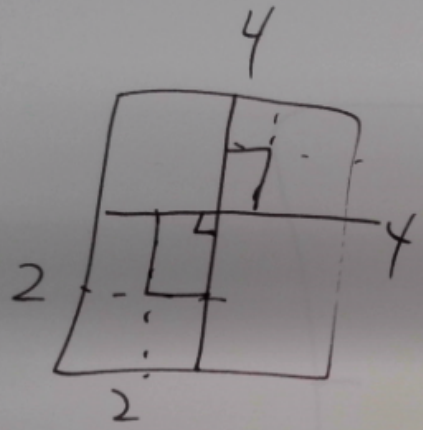


$\therefore P(n+1)$

$\therefore P(n) \; \forall n \geq 1$


1024
1024
512
512


512
512
256
256


4
4
2
2