Brain Teaser (pay attention!)

- A school principal does an experiment
- 1000 students are lined up in front of 1000 lockers, which are all shut
- The first student opens every locker
- The second student starts at locker 2, and takes every other locker
  - If it's closed, she opens it, and if it's open, she closes it.
- The kth student visit every kth locker changing its "state"
  - open->closed, closed->open
- After 1000 students pass through, which lockers are closed?

Mathematical Induction

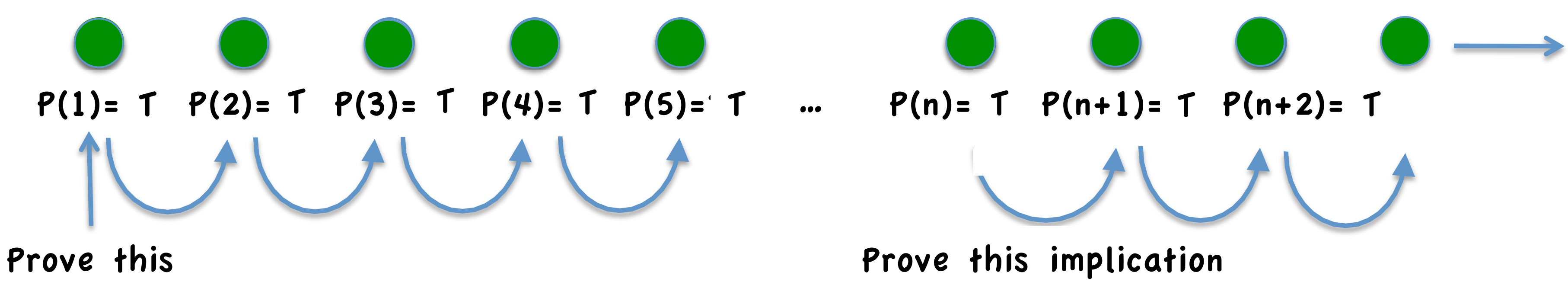
- <u>Induction:</u> inference of an event from past events
- In math, use property of ints 1-999 to infer property of 1000.

Positive Integers

- The set of positive integers
  - $Z^+ = \{1, 2, 3, \ldots\}$
- The set of negative integers
  - $Z^- = \{-1, -2, -3, \ldots\}$
- Zero is neither positive nor negative

Principle of Mathematical Induction

- Define a predicate P(n) on the set of positive integers
- Prove the following implication
  - $P(n-1) \rightarrow p(n) \ \forall \ n \in N$
- This implication allows you to hop your way from one to infinity



“Four-Step” Plan

To prove a statement of the form:

“P(n) s true for all natural numbers n.”

1. <u>Problem Statement</u>: Formulate P(n)
2. <u>Base Case</u>: Prove P(1) is true
3. <u>Inductive Hypothesis</u>: Assume P(n) for some n
4. <u>Inductive Step</u>: Prove P(n+1) is true

Closed Expressions for Sums

- Prove:

$$S(m) = \sum_{i=1}^{m} i = 1 + 2 + 3 + \ldots + m - 1 + m$$
$$= \frac{m(m+1)}{2}$$

- What are the steps?

Inductive Proof of Sums

- $S(1) = 1$ (by definition)
  - and $1(1+1)/2 = 1$ (by formula)
- By definition: $S(m+1) = S(m) + m+1$
  - Recursive expression of sum
- Now deploy the inductive assumption
  - $S(m) = m(m+1)/2 \rightarrow S(m+1)$

  $= m(m+1)/2 + m+1 = (m^2+m + 2m+2)/2$

  $= (m^2+3m+2)/2 = (m+1)(m+2)/2$ (closed form)
- Therefore, $S(m) = m(m+1)/2$

Practice

- For:
  - $a(k) = a(k-1) + 2k$
  - Prove that $a(n)=n(n+1)$
- For
  - $S(n) = 1+3+5+\ldots+(2n-1)$
  - Prove that $S(n)=n^2$

Another Example

- **Prove:** $S(n) = \sum_{i=1}^{n} \frac{2}{3^i} = 1 - \frac{1}{3^n}$

- **S(1) = 2/3 (definition)**
  - **= 1-(1/3)=2/3 (closed form)**
- **Recursive form**

$$S(n+1) = S(n) + \frac{2}{3^{n+1}}$$

$$= 1 - \frac{1}{3^n} + \frac{2}{3^{n+1}} = 1 - \frac{-3+2}{3^{n+1}} = 1 - \frac{1}{3^{n+1}}$$

Closed form for S(n+1), we done

Inductive assumption

Common denominator and reduce

Proving Other Things

- Number sequence: $a(n) = 2a(n-1)+a(n-2)$
- $a(1)=5$, $a(2)=10$
- Prove that $a(n)<3^n$ for all $n\geq3$
- $P(3)=2\cdot10+5=25 < 3^3=27$
- $P(4)=2\cdot25+10=60 < 3$^$4=81$
- Assume: $a(n)<3^n$ and $a(n-1)<3^{(n-1)}$
- Then $a(n+1) = 2\cdot a(n)+a(n-1)$
    - $< 2\cdot3^n+3^{(n-1)}$
    - $< 2\cdot3^n+3^n = 3^{(n+1)}$ (which satisfies the property)
- Done

Fibonacci Numbers

- $f(1)=1$, $f(2)=1$
- $f(n)=f(n-1)+f(n-2)$
  - 1,1,2,3,5,8,

Fibonacci Numbers

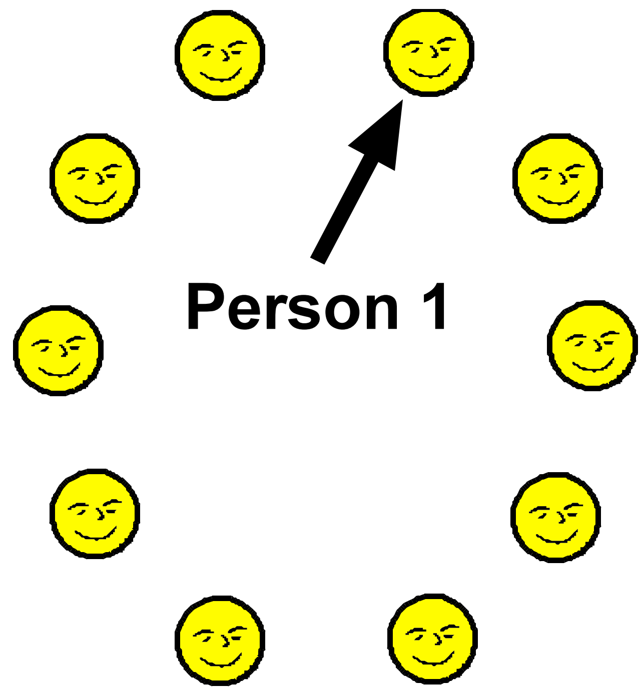
- Prove that if 3|n, then f(n) is even
- f(3)=2, which is even
- Assume f(n) is even and 3|n. Show f(n+3) even.
  - Strategy, think of 3|n as a sequence
  - …f(n-3), f(n), f(n+3)…
- Cases:
  - f(n-1) is even. Then f(n+1) is even, because even numbers are closed under addition
    - -> f(n+2) even, f(n+3) even
  - f(n-1) is odd, then f(n+1) is odd, because even+odd is odd.
    - ->f(n+2) is odd, because f(n+2)=f(n+1) *[odd]* + f(n) *[even]*
    - ->f(n+3) is even, because f(n+3)=f(n+2) *[odd]* + f(n+1) *[odd]*
- Therefore, f(n+3) is even, and (f(n) even)->(f(n+3) even)

A matter of life and death

In the Jewish revolt against Rome, Josephus and 39 of his comrades were holding out against the Romans in a cave. With defeat imminent, they resolved that, like the rebels at Masada, they would rather die than be slaves to the Romans. They decided to arrange themselves in a circle. One man was designated as number one, and they proceeded clockwise killing every seventh man... Josephus (according to the story) was among other things a mathematician; so he instantly figured out where he ought to sit in order to be the last to go. But when the time came, instead of killing himself he joined the Roman side.

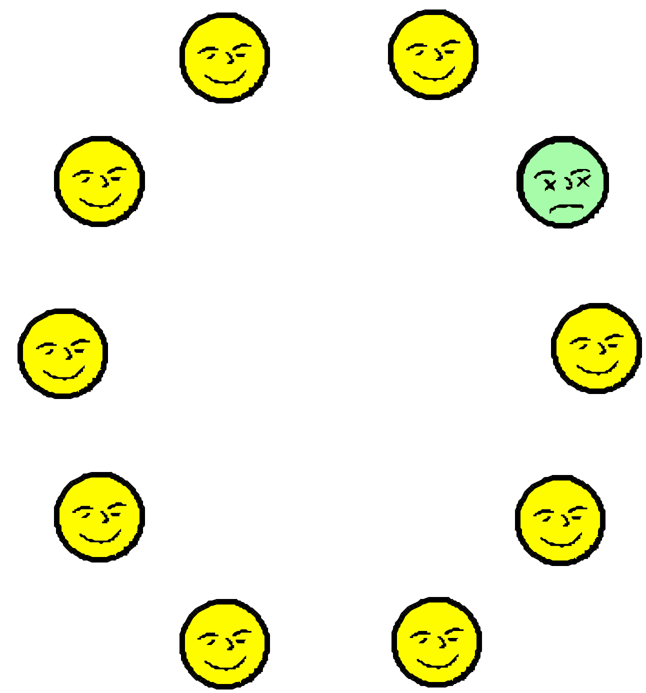
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



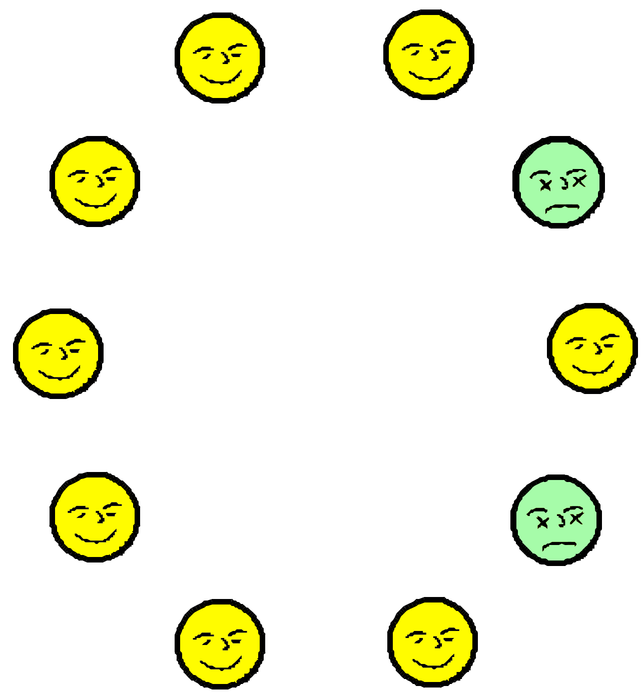
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



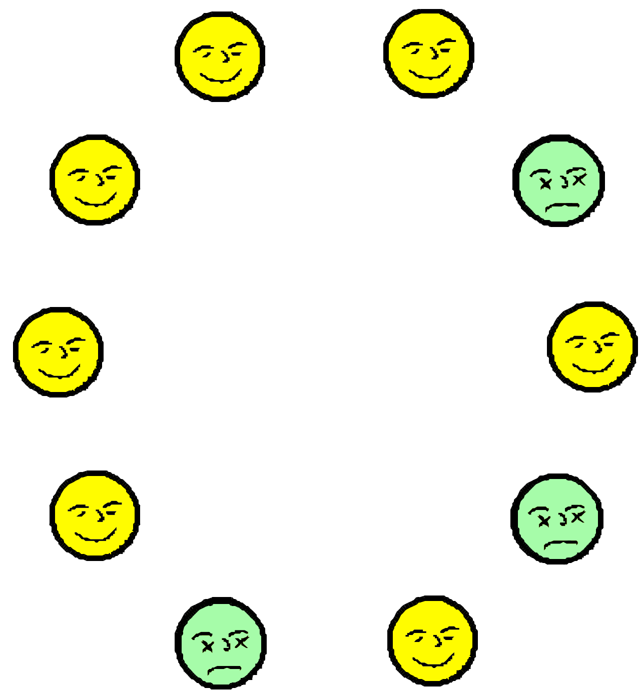
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



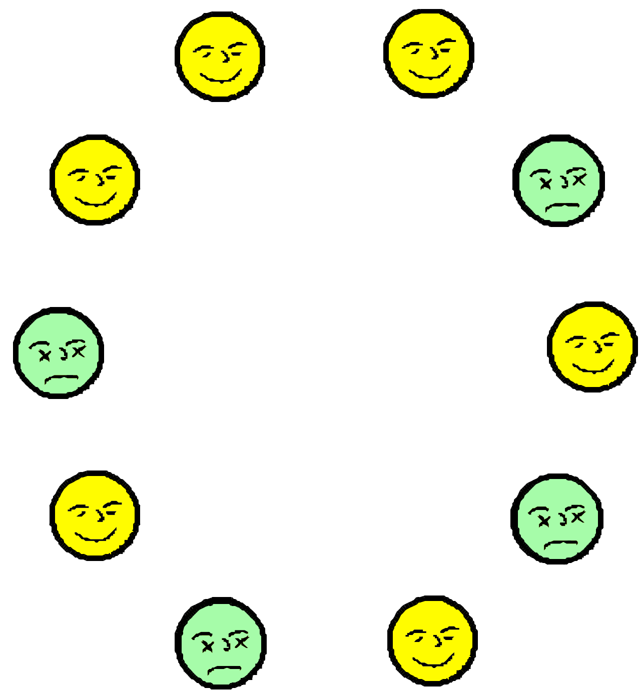
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



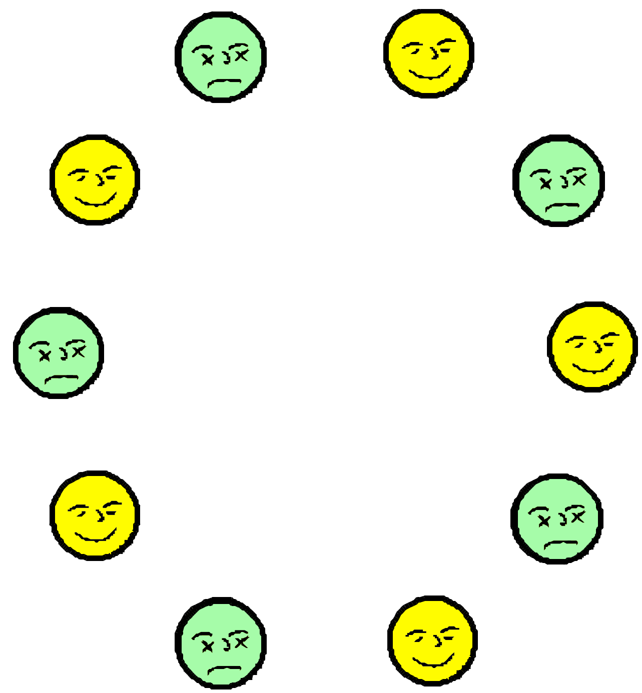
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



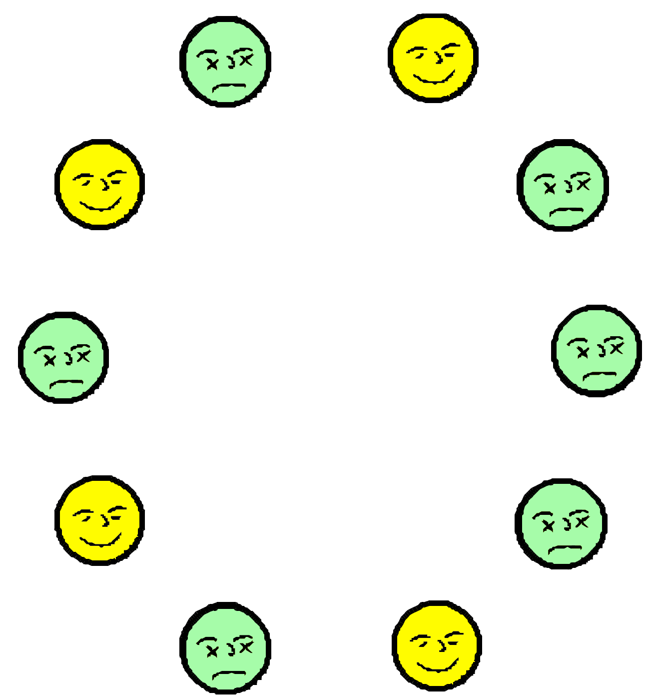
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



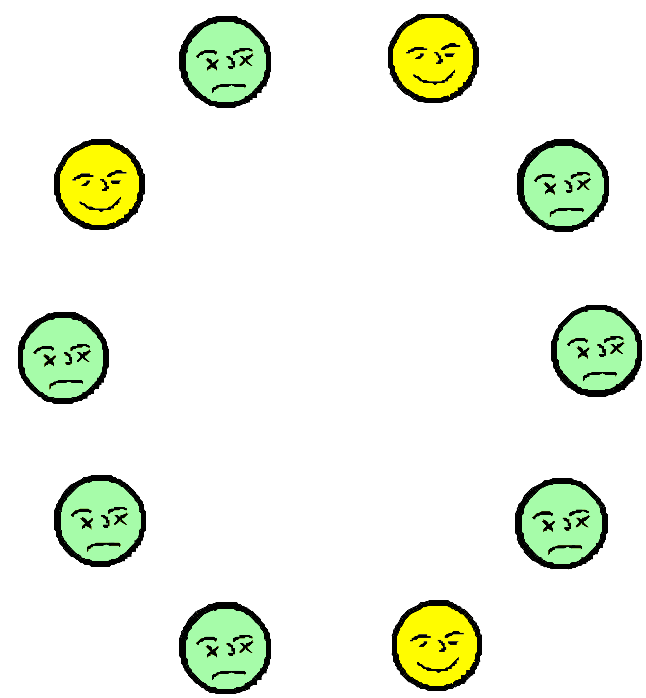
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



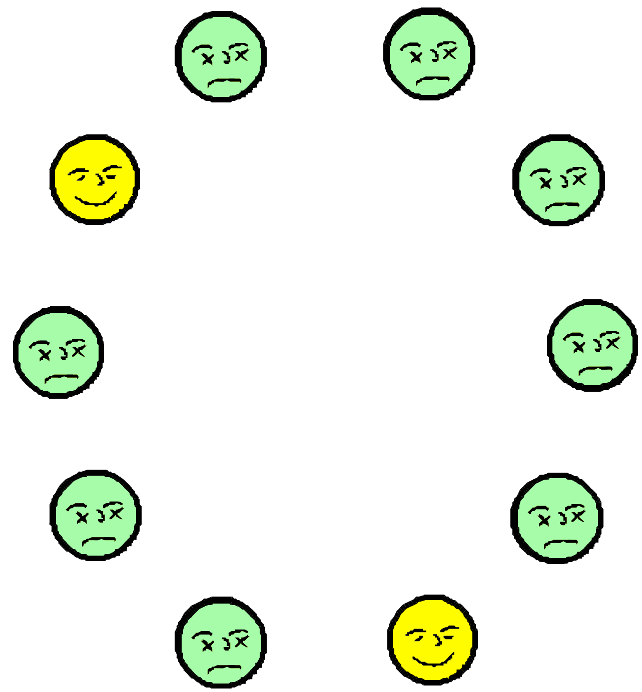
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



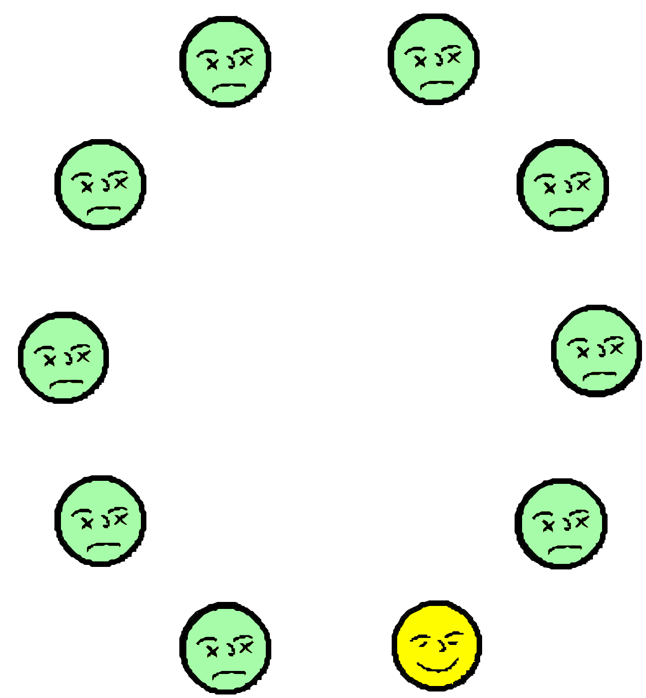
Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



Josephus 2x

If there are 10 people numbered 1 to 10 in a circle, and every other person is killed starting with number 2, which person is left?



Josephus 2x Theorem

- P(n): For a 2^n person, 2x game, the winning strategy is to be in position 1.
- P(2): the second person is killed and then the first.
- P(n+1): for $2^{(n+1)}$ people, every other person starting with 2 and ending with $2^{(n+1)}$ is killed.
  - Therefore, the game continues with the first person again and 2^n players.
- ∴P(n) -> P(n+1), and the theorem is proven

Contradiction and Pigeonhole Principle

- Methods of proving:
  - Direct proof
  - Proof by contrapositive
  - Mathematical induction
- Prove by contradiction
  - There cannot possibly be a counter example to the theorem.
  - Such an example must
    - Make the hypothesis true
    - Make the conclusion false

Example

- If n^2 is odd, then n is odd.

Direct	**Contrapositive**
Let n^2 be an odd integer	Let n be even
$\vdots$	$\vdots$
We conclude that n is odd	We conclude that n^2 is even

Contradiction
Suppose there is an integer n such that n^2 is odd and n is even
$\vdots$
We infer a false statement.
This is a contracition, so such a counter example cannot possibly exist.

Example

- Prove: $\forall x \in R$, $(x>0) \rightarrow (1/x)>0$
- Suppose there is a counterexample, with $x>0$ and $(1/x)\le 0$
- Because x is positive we have
  - $(1/x)\le 0$
  - $x \cdot (1/x)\le x \cdot 0$
  - $1\le 0$
- This cannot be true, so there must be no counter example

Existence and Nonexistence

- Existence
  - There exists x s.t. P(x)
    - Easy proof: find an example
  - Constructive proofs
    - Show how an example satisfies the condition
- Nonexistence
  - The existence leads to an contradiction

Relatively Prime

- Two numbers are relatively prime iff they have no common divisor greater than 1.
  - Examples (relatively prime or not?)
    - 20, 6
    - 21, 8
    - 56, 15
    - 49, 14

Thereom

- Any rational number can be written as a ratio of relatively prime numbers
- Proof (construction):
  - let r=a/b and let a,b share a factor c
  - $r=(c \cdot d)/(c \cdot e)=d/e$
  - The number of factors a number has in finite, so we can repeat the above process until the two numbers are relatively prime.

Nonexistence Proof

- sqrt(2) is not rational
- Suppose sqrt(2) is rational
  - Then $\exists$ $r \in Q$, $r^2=2$
  - ->$(a/b)^2=2$, where a,b are relatively prime
  - -> $a^2=2b^2$ -> a is even, $a=2k$
  - -> $a^2=4k^2=2b^2$
  - -> $b^2=2k^2$ -> b is even
  - -> a,b are both even
  - -> a,b share a factor of 2
  - -> they are not relatively prime

Fundamental Theorem of Arithmetic

- Every integer greater than 1 can be expressed as a product of prime numbers
- Proof:
  - By induction, with the proposition that all numbers $< n$ can be expressed so
  - Cases:
    - n – prime
    - n – not prime

Example: Proof by Contradiction

- <u>Theorem: </u>There are an infinitely many prime numbers
- Proof:
  - Assume there are only k prime numbers, the biggest l
  - Then we can multiply them all together and get a bigger number, q>l
  - p=q+1 has a remainder of 1 for all the primes
  - By the fund. thm. of arithmetic, any factor of p can be further factored into primes.
    - But no primes>1 divide p, so it must be prime
  - -> p must be prime
  - This is a contraction because p was not in the original set

A Game

- You give 29 tennis balls out to four players.
  - One player has the most (or tied) balls
  - What is the least number of balls she could have?

The Pigeonhole Principle

- If $m \cdot n+1$ objects are distributed among n containers, then there must be some container containing at least $m+1$ objects

The Pigeonhole Principle

- Proof (by contradiction):
  - $x(i)$ = number of objects in container I
  - $x(1)+x(2)+\ldots+x(n)=m \cdot n+1$
  - The counter example: $\forall i,\ x(i) \leq m$
  - -> $x(1)+x(2)+\ldots+x(n) \leq m+m+\ldots+m = n \cdot m$
  - but $x(1)+x(2)+\ldots+x(n)=m \cdot n+1$
  - so we have a contradiction
- $\therefore$ for n containers to hold $n \cdot m+1$, there must be a container m+1 or more objects

Proposition and Proof

- Given any 4 integers in Z^+, some pair of them will have a difference divisible by 3
- Put each number k into one of 3 boxes
  - Labeled 0,1,2
  - The box number is the remainder of $k \div 3$
  - Some box, d, contains at least 2 numbers
    - Call them a & b
  - $a=3J+d$, $b=3L+d$
  - -> $a-b = 3J+d-3L-d = 3(J-L) = 3M$ $(M \in Z)$
  - QED

Practice Problem

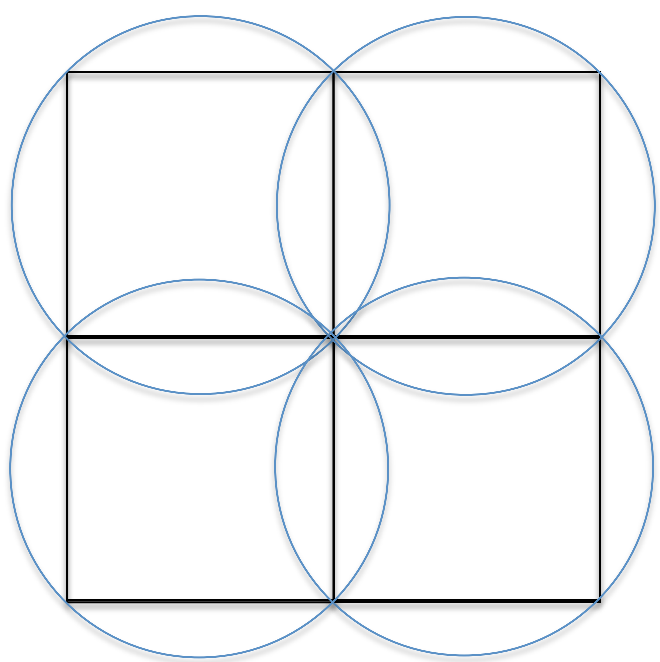
- For any 11 positive integers, some pair of them must have a difference divisible by 10.

Proposition and Proof

- Given any 5 points placed in the unit square, there must be at least 2 placed within sqrt(2)/2 of each other
- Proof
  - Divide the square into four equal squares
  - Each square is contained in a circle of diameter sqrt(2)/2
    - Any two points in that circle are at most sqrt(2)/2 apart

Proposition and Proof

- By PHP, at least one square must contain two points
- Those two points are contained in the same sqrt(2)/2 circle



What configuration of five points achieves this optimum?