There is a hallway with 50 switches numbered 1 to 50, which are all in the off position. 50 people pass down the hallway. The first person flips every switch (turning them all on). The second person flips the switches whose numbers are a multiple of 2 (turning them off again). The third person flips the switches whose numbers are a multiple of 3 (turning some off and some on). This continues until all 50 people pass through, the last one only flipping the 50th switch.

At the end, which lights are on, and which are off?

$1 \qquad d \qquad \sqrt{n} \qquad n/d \qquad n$

Today Ch. 4 & 6

Axioms of counting #s (Peano Axioms)

$\mathbb{N}$ has a special "successor" procedure which takes a number n and gives the "next" number $S(n)$

Natural #s is a collection of things we call numbers w/ a procedure S such that

- if n a number $S(n)$ is also
- if $S(n)=S(m)$ then $n=m$
- there's a # 0 such that $0 \neq S(n)$ any n.
- "Principle of induction"

Q: How do we know this makes sense?

A: Gödel says: can't know.

Next best thing: Agree to trust some Axiom system and go from there. **Set theory**

If Set theory makes sense then we can model arithmetic w/ sets & show Peano axioms make sense.

Procedure: construct #s **as sets**

to make this infinite: $n \longleftrightarrow$ set w/ n elements.

$0 \equiv \emptyset$

$1 = \{0\}$

$2 = \{0,1\}$

$3 = \{0,1,2\} = \{0,1\} \cup \{2\}$

$= 2 \cup \{2\}$

$n+1$

$S(n) = n \cup \{n\}$

$0 = \emptyset \quad 1 = \{0\} = \{\emptyset\}$

$2 = \{0,1\} = \{\emptyset, \{\emptyset\}\}$

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

in textbook $\mathbb{N} = \{1, 2, 3 \ldots\}$
in class $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$

Prime numbers

Definition Given natural numbers (integers) a, b we say that b is divisible by a (or that a divides b) if we can write $b = da$ for some natural number (integers) d.

in this case, we write $a \mid b$ "a divides b"

- $\overset{b}{0}$ is divisible by anything $a \mid 0$ since $0 = 0 \cdot a$
- 1 divides every number $1 \mid b$ since $b = b \cdot 1$

ex: $6 \mid 42$ $42 = 6 \cdot 7$ $42 = 2 \cdot 3 \cdot 7$

$6 = 2 \cdot 3$

factoring

2, 3, 7 "building blocks" of 42

Q: what are the basic building blocks of #s ?

- $2 = 2$
- $3 = 3$
- $4 = 2 \cdot 2 = 2^2$
- $5 = 5$
- $6 = 2 \cdot 3$

⋮

- $91 = 13 \cdot 7$
- $93 = 31 \cdot 3$
- $23212 = 2 \cdot 2 \cdot 7 \cdot 829$

Def A number is called prime if it is a natural number greater than 1 such that the only natural numbers which divide it are 1 and itself.

Q: How many prime #s are there?
if infinite then (as described) countably infinite.

Euclid: why there are infinitely many prime #s.
If there were only finitely many, could list them
$p_1, p_2, \ldots, p_n$ complete list.

$m = p_1 p_2 p_3 \cdots p_n + 1$ if this was prime then it wasn't on list since it's (much) bigger than anything on list!

so this is impossible.
So this number isn't prime.

we break up m (factor it) and at the end the pieces (factors) are the numbers $p_1, p_2 \ldots$

$\Rightarrow m = p_i(\quad)$ $\qquad p_i \mid m$

but when we divide m by p_i always get a remainder of 1!

so m isn't divisible by

any of the ones on list!

Division

"The division algorithm"

Fact: for any integers a & b there exist unique natural #s d, r with $b = ad + r$ where r is a natural number with $r < |a|$

ex: "$42/5$" $42 = 5 \cdot 8 + 2$

$2 < |5|$

ex: Even & Odd

we say a number is even if it has a remainder of 0 when divided by 2.

— — — odd — — — — — 1

— — — — 2.

Random proofs:

every number greater than 2 is the sum of a multiple of 3 & an even number.

a nat #
(0 or bigger)

proof: if $n \geq 2$ divide by 3

$n = 3d + r$

$0, 1, 2$

✓ ✓

$n = 3d + 1$

$= 3(d-1) + 3 + 1 = 3(d-1) + 4$

$n = 0 + 1$ can't happen ! $n \geq 2$.

"Digression" The parity number system.

odd o

even e

$e + e = e$ $e + o = o$

$ee = e$ $o + o = e$

$eo = e$ $oo = o$

$e(o+o) = eo + eo = e + e = e$

"

$e(e) = e$

10-arity arithmetic:

$[0]_{10}$ 0 ish — rem 0 when div by 10

$[1]_{10}$ 1 — 1

⋮

$[9]_{10}$ 9 is

53 is $[3)_{10}$ type #.

$$[3]_{10} + [6]_{10} = [9]_{10}$$

3	$[3]_{10}$
6	$[6]_{10}$
9	$[9]_{10}$

$$[7]_{10} + [8]_{10} = [5]_{10}$$

n m

$n = 10 \cdot d + 7$

$m = 10 \cdot e + 8$

$n + m = 10(d+e) + 15$

$= 10(d+e+1) + 5$

$$[3]_{10} \cdot [6]_{10} = [8]_{10}$$

$[7]_{12} + [11]_{12} = [6]_{12}$

modular arithmetic (base 12)

These let you see fun arith. facts

432 591

3003

$$\begin{array}{r} 300 \\ +3\cdot 5 \\ \hline 315 \end{array}$$

$$\begin{array}{r} 31 \\ 25 \\ \hline 56 \end{array}$$