$$\pi = 3 + 0.1415\ldots$$

$$= 3 + \frac{1}{7.0625\ldots}$$

$$= 3 + \frac{1}{7 + 0.0625\ldots}$$

$$= 3 + \frac{1}{7 + \frac{1}{15.996\ldots}}$$

Continued fraction expansion

3

$$3 + \frac{1}{7} = \frac{22}{7}$$

$$3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106}$$

etc.

$$\frac{17}{39} = 0 + \frac{1}{39/17}$$

loop:
$x \leftarrow x - \lfloor x \rfloor$
$x \leftarrow 1/x$

$$= 0 + \frac{1}{2 + 5/17}$$

$$= 0 + \frac{1}{2 + 1/(17/5)}$$

$$= 0 + \frac{1}{2 + \frac{1}{3 + 2/5}}$$

$$= 0 + \frac{1}{2 + \frac{1}{3 + 1/(5/2)}} = 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2 + 1/2}}}$$

✓

$$0 = 0$$

$$0 + \frac{1}{2} = \frac{1}{2}$$

$$0 + \frac{1}{2 + \frac{1}{3}} = \frac{3}{7}$$

Convergents hope for $\in \frac{1}{n}\mathbb{Z}$

Hidden Subgroup Problem

G - group
H - subgroup

$f: G \to X$

w/ property $f(g_1) = f(g_2) \iff g_1 - g_2 \in H$

Goal: Determine H

Shor's example

$$f: \mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$
$$x \longmapsto a^x \bmod n$$

$$f(g_1) = f(g_2) \iff a^{g_1} = a^{g_2}$$
$$\iff a^{g_1 - g_2} = 1$$
$$\iff g_1 - g_2 \in r\mathbb{Z}$$

Discrete Log in $\mathbb{Z}/p\mathbb{Z}$ $(h = g^x)$

$$f: \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^*$$
$$f(\alpha, \beta) = h^\alpha g^{-\beta}$$

$$f(\alpha_1, \beta_1) = f(\alpha_2, \beta_2)$$
$$\iff h^{\alpha_1} g^{-\beta_1} = h^{\alpha_2} g^{-\beta_2}$$
$$\iff h^{\alpha_1 - \alpha_2} g^{-(\beta_1 - \beta_2)} = 1$$
$$\iff h^{\alpha_1 - \alpha_2} = g^{\beta_1 - \beta_2}$$
$$\iff x(\alpha_1 - \alpha_2) \equiv \beta_1 - \beta_2 \pmod{p-1}$$

$$(\alpha_1, \beta_1) - (\alpha_2, \beta_2) \in \{(\alpha, \beta) : \beta = x\alpha \bmod (p-1)\}$$

Error Correcting Codes

why: noisy channels

model: sending bits over a channel with probability p that a bit is flipped.

Basic Example

message: 1 bit

encoded message: repeat 3 times.

bit to send	encoded codeword
0	000
1	111

This code can
* detect 2 errors
* correct 1 error

ex. if $p = 0.1$

this is 0.972

Suppose we send codeword 000

received	# errors	error detected?	decoded
000	0	0	000 ✓
001	1	1 ✓	000 ✓
010	1	1 ✓	000 ✓
100	1	1 ✓	000 ✓
011	2	1 ✓	111 ✗
110	2	1 ✓	111 ✗
101	2	1 ✓	111 ✗
111	3	0	111 ✗

Probability of correctly decoding:

$$(1-p)^3 + (1-p)^2 p + (1-p)p(1-p) + p(1-p)^2$$

no error; error only in 1st bit; 2nd; 3rd

$$= (1-p)^3 + 3p(1-p)^2$$

Parity Check Code

message: 7 bits

Encoded message: add 1 bit = parity of the sum of the other 7

eg. message: 0110001

encoded: 01100011

Σ $1+1+1 \equiv 1 \pmod 2$

a codeword $\iff$ Σ digits is even

Can detect one error

no errors corrected

But: message is inflated a lot less.

Fundamental challenge:

detect & correct as many errors as possible

without too much inflation

also: efficient

Def^n. Let $\mathcal{A}$ be an alphabet.
and let $\mathcal{A}^n$ = n-tuples from $\mathcal{A}$.

A **code of length n** is a non-empty subset of $\mathcal{A}^n$.

The elements are called codewords.

If $|\mathcal{A}| = 2$, "binary code"
$|\mathcal{A}| = 3$, "ternary code"
$|\mathcal{A}| = q$, "q-ary code"

1st Example. (triple repeat)

$\mathcal{A} = \{0,1\}$

code $= \{(0,0,0), (1,1,1)\} \subseteq \mathcal{A}^3$

length 3 binary code.

8 bit Checksum (2nd ex.)

$\mathcal{A} = \{0,1\}$

code $= \{$ 8 bit strings w/ $\sum$ bits = even $\} \subseteq \mathcal{A}^8$

length 8 binary code.

Def^n Let $u, v \in \mathcal{A}^n$.

The Hamming distance $d(u,v)$ = # of positions where u & v differ.

eg. $u = (1,0,1,1,0)$ and $v = (1,1,1,0,0)$

then $d(u,v) = 2$.

Typically, decoding means finding the codeword at closest Hamming distance from the received message.