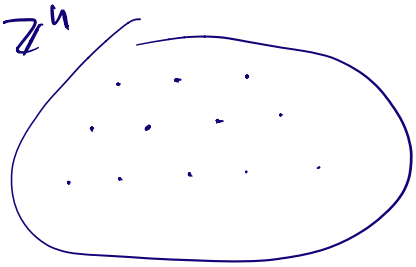
Algorithmic Number Theory

Some problems

1. Algorithms for arithmetic
   $+, \times$, other stuff
   representations
2. Primality testing
3. Factoring integers
4. Discrete logs
5. Polynomial analogues of all these
6. Lattices eg $\mathbb{Z}^n$



7. Recognizing algebraic numbers.
8. Elliptic Curves

9 Cryptography and motivations From there

10. Hilbert's 10th problem.
Undecidability of solvability of Diophantine equations.

11. Quantum Algorithms

Problem sets

Project at the end 10-15 page write up on a recent research paper.

Generalities

Represent integers in base 2.

1. Can add, multiply, divide, subtract, convert bases in time poly(n) where the inputs are n-bits long.

2. Rational numbers, represented as

$a/b \qquad a, b \in \mathbb{Z}$.

"Complexity" of $a/b \triangleq \log_2(a) + \log_2(b)$

---

2 problems

1. GCDs: computing GCD of 2 numbers
2. Recognizing approximate rational numbers.

Baby algorithm for GCD (a, b)

(1) factor a, b

(2) use prime factorization.

Factoring is difficult!

- Trial division requires time $\geq \left(2^{n/2}\right)$

Euclid's GCD algorithm

Observation: $GCD(a,b) = GCD(a-b,b)$
$= GCD(a \bmod b, b)$

Alg (a,b):
Make $a > b$ by swapping a, b if necessary.
If $b = 0$
return a
else
return Alg $(a-b, b)$
Alg $(a \bmod b, b)$

—

$a > b$
$\log a + \log b$ keeps reducing by
vs
$\log (a \bmod b) + \log b$.

Claim: $(a \bmod b) \cdot b < \frac{a \cdot b}{2}$.

If $a > 2b$, then yes.

If $a = (1+\alpha)\cdot b$

then $a \bmod b = \alpha b < \left(\frac{1+\alpha}{2}\right) b.$

So Alg (a,b), if a, b are n bit long integers, runs in $\leq 2n$ recursions.

Runtime of Alg $\leq O(n^3)$.

Bezout Identity

If $GCD(a,b) = d$,

then $\exists\ x, y \in \mathbb{Z}$ s.t.

$$ax + by = d.$$

Can also find x, y like this using Euclid's algorithm.

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$r_{s-1} = q_{s+1} \cdot r_s + d \quad (= r_{s+1})$$

$$r_s = q_{s+2} \cdot d + 0$$

$$(= r_{s+1})$$

This gives us d as integer combination of a, b.

$\longrightarrow$

Given relatively prime a, b,

can find x s.t. $ax \equiv 1 \bmod b$.

[Find x, y s.t. $ax + by = 1$.

Then $ax \equiv 1 \bmod b$]

Continued FRACTIONS

$$1.73 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

where all $a_i \in \mathbb{Z}$

$a_i > 0$.

$a_0 = 1$

$$\frac{1}{0.73} = a_1 + \cfrac{1}{\ddots}$$

$$1.3 = 1 + \cfrac{1}{\ddots}$$

$$\frac{1}{0.3} = a_2 + \cfrac{1}{\ddots}$$

$$3.1 = 3 + \cfrac{1}{\ddots}$$

$$1.73 = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{\ddots}}}$$

Problem Given rational number $\frac{a}{b}$,
and a denominator bound Q,
where a, b, Q are all $\leq n$ bits long.
find p, q s.t.

$\left| \frac{a}{b} - \frac{p}{q} \right|$ is minimized over all
rationals $\frac{p}{q}$ with $q \leq Q$.