An Overview of Integer Factorization Algorithms

NAKKUL SREENIVAS

Practical Applications and Uses

- Primes are the basis of modern day encryption schemes. Why?
  - No factors which makes it harder to decrypt without knowing the exact prime value. Refer to Polyalphabetic cipher
  - Fewer collisions when encrypting.
  - Hard to generate large primes (with exception of certain special primes i.e. Mersenne Primes etc.)
- For most intents and purposes prime factorization is the same problem as prime generation.
- Used for public key generation (RSA encryption) by multiplying two large primes with one being a key.

Types of Algorithms

- Category 1
  - Pollards Rho, Fermat, Euler
- Category 2
  - Dixons, GNFS, Quadratic, Shanks
- Special Cases
  - Shor’s

Upper bound for Worst Case Runtime

- Runtime based on size of integer **N**.
- Brute force (Sieve of Erastosthenes) gives a lower bound of $\sqrt{n}$.
- Include basic optimizations of the sieve $\sqrt{n}/\log(n)$.
  - Store in table
  - Start at the square of the number

Quadratic Sieve

- Fermat's Factorization method
- Searching for values of **p** and **q**.
- Comparative speed and run time:
  - $O(e^{\sqrt{\ln(n)\ln(\ln(n))}})$
  - Fastest algorithm for numbers up to about 10^{100}

$$N = 255$$
$$\therefore a = \sqrt{255} = 15.9687... = 16$$

$$b = \sqrt{(a^2 - N)}$$
$$\therefore b = \sqrt{(256 - 255)}$$
$$\therefore b = 1$$

$$a + b = 17$$
$$a - b = 15$$

General Number Field Sieve

- Works similar to the quadratic sieve
- Includes an optimal strategy for choosing p and q using **smooth numbers**
- Assigns each number to a vector given its prime factorization.
  - Uses these numbers to search for the proper p and q in form using linear algebra (matrix reduction)
- Computationally very intensive
- Requires huge amounts of memory but is faster for extremely large values of **n**.

Non-Sieve Algorithms

- CFRAC –Lehmer and Powers
- Dixon's- John D. Dixon
  - Uses a weaker assumption but with limitations
- Shanks' Method (congruence of squares and Fermat's)

Alternate Algorithms

- Other algorithms can be useful for reasons apart from cryptography
- If not searching for a number comprised of two large primes, can use a category 1 algoritm
- Most calculators use a variant of Pollard Rho’s algorithm.
- Other methods include Fermats and Euler’s methods.

Recent Advancements

- Three Taiwanese mathematicians developed a variant of Fermat's algorithm to search for factors in a more efficient manner.
- Used the technique of continued fractions and optimized a method to eliminate loop counts.
- Success rate of approximately 81.7% with large composite numbers.

Recap and Related Topics

- Integer Factorization relevance
- Advancements
- Shor’s algorithm