MATH 314 Spring 2019 - Class Notes

Scribe: Josh Robertson

4-18-2019

Dixons Factorization Algorithm
Evolved from “Quadratic Sieve”

- Idea: Use the Factoring Trick
- Goal: Find two numbers where:

  $a \neq \pm b$ (mod n)
  $a^2 = b^2$ (mod n)

1. Pick prime number bound $B \approx e^{\sqrt{ln(n)}}$
   - We’re looking for numbers all of whose prime factors are less than B. These are called B-Smooth numbers.
   - For example: $B = 6$; 30 is 6-smooth: $30 = 2 \times 3 \times 5$ (all factors less than 6)
   - 42 is not 6-smooth: $2 \times 3 \times 7 >> (7 > 6)$
2. Pick a random “a” with $\sqrt{n} < a < n$
3. Compute a^2 (mod n)
   - If result is B-smooth, we keep it
   - If not, repeat with different a
   - We need a bunch of a’s that work out.

   Let P be the number of primes less than B. Wait until we have P+1 values, where a^2 (mod n) is B-smooth.
4. Take these values of a, write out the prime factorization of a^2 (mod n)
   - Make a matrix where every column is one of the prime numbers less than B and each row is each value of a
   - Entries in the matrix are the number of times that prime divides a^2 (mod n)
5. By linear algebra because there are more rows than columns there must be some combination of rows that we can add together to get all even numbers. Since all exponents are an even number the integer we get by multiplying together the corresponding a^2 values is a square.

Lets suppose $a_1, a_2, ..., a_k$ were the values of a used to make this even combination

Let $x_1 = (a_1)^2$ (mod n)

$x_2 = (a_2)^2$ (mod n)

●●●

$x_k = (a_k)^2$ (mod n)

Then $x_1 \times x_2 \times ... \times x_k = X$ where X is a square. So $\sqrt{x} = y$ is an integer.

Thus $x^2 = X = x_1 \times x_2 \times ... \times x_k = a_1 \times a_2 \times ... \times a_k$ (mod n)

$y^2 = (a_1 \times a_2 \times ... \times a_k)^2$ (mod n)

We found that $y^2 = A^2$ (mod n),

usually with $y = \pm A$ (mod n)