Primes

ian.mcloughlin@gmit.ie

PRIMES

Definition

$$PRIMES = \{2, 3, 5, 7, 11, 13, ...\}$$

PRIMES is the set of all primes numbers.

Can a Turing Machine be designed to decide PRIMES? (Yes)

Some people say PRIMES is the decision problem for the set of primes.

Can it do it in polynomial time? (Yes)

Is PRIMES in P? (Yes, 2002)

www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf

Modern cryptography

Modern asymmetric key cryptography is based on prime numbers

It depends on two facts:

- It's easy to verify primes (P).
- It's hard to decompose a composite number into primes (Not known to be P).

Generating versus verifying

Note that it's not necessarily easy to generate prime numbers. We know that verifying a number is prime can be done in polynomial time. That doesn't mean that we can generate prime numbers in polynomial time. You must start with the prime, and then ask the question.

Brute force prime checking

Is n a prime?

```
function is_prime(n) {
  for (var i = 2; i < n; i++) {
    if (n % i == 0)
      return false;
  }
  return true;
}
```

More efficient prime checking

- Suppose $a \times b = n$.
- Then $a < b$, $a > b$ or $a = b$.
- No matter what, $a \leq \sqrt{n}$ and/or $b \leq \sqrt{n}$.
- So only loop to $\sqrt{n}$.
- This still isn't that efficient.

Slightly more efficient

Is n a prime?

```
function is_prime(n) {
  for (var i = 2; i < Math.sqrt(n); i++) {
    if (n % i == 0)
      return false;
  }
  return true;
}
```