Theorem and algorithm of Agrawal, Kayal, Saxena

Carola Behr for Proseminar on prime numbers and cryptography April 2022

"We present a deterministic polynomial time algorithm that determines whether an input number n is prime or composite."
(Abstract of "PRIMES is in P" by Agrawal, Kayal, Saxena)

This talk will cover the algorithm to determine whether an integer is a prime or is composed by Agrawal, Kayal and Saxena and give some background on previous attempts to find such an algorithm.

Tools to check result of primality test

- If n prime all numbers smaller than n are coprime ("teilerfremd") to n
- n prime $\Longrightarrow n-1$
  values mod n which are coprime to n
- These values form a cyclic group with multiplication
  $\Longrightarrow$ there is a generator g of this group with $ord(g) = n-1$
- If g not generator then there is a prime $q \leq n-1$ with $q|n-1$ for which $g^{\frac{n-1}{q}} = 1\ (mod\ n)$
- with $Q = \{q: q\ prime\ and\ q|n-1\}$ and a generator g one can check a given integer n is prime
- Need to check $g^{n-1} \equiv 1\ (mod\ n)$ and $g^{\frac{n-1}{q}} \not\equiv 1\ (mod\ n)\ \forall\ q \in Q$
- So primality tests are in NP
- This is not algorithm we look for, as we would have to factor n-1, only checking is "easy"

Wilson's Theorem (1770)

- integer $n \geq 2$ is prime $\Leftrightarrow$n divides $(n-1)!$ +1
- Difficult to convert into algorithm as $(n-1)!$ is hard to compute

Fermat (1637)

- Known Binomial theorem:
  $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$
- In fields K with $char(K) = p$ (p a prime):
  $(x+y)^p = x^p + y^p$
- Characterisation of primes:
  - p prime $\Rightarrow p|a^p - a\ \forall a \in \mathbb{Z}$
  - p prime $\Rightarrow a^p \equiv a\ (mod\ p)$
- Problem: there are also composites for which this holds

Square roots

- 1 has at most 2 square roots in $\mathbb{Z}/_{p\mathbb{Z}}$ $(p\ a\ prime)$:
  1 and $-1\ \equiv p-1$
- 1 has at least for different square roots in $\mathbb{Z}/_{n\mathbb{Z}}$ (n an integer composed of at least two different primes)
- Call $a \in \mathbb{Z}$ a witness to n if the sequence $a^{n-1}\ (mod\ n)$, $a^{\frac{n-1}{2}}\ (mod\ n)$, $a^{\frac{n-1}{4}}\ (mod\ n)$, …. Does not reach $1\ or\ -1$
- Can show that at least half of the numbers smaller than n are witnesses
- Test numbers to find witness produces „industrial strength prime"

Agrawal, Kayal, Saxena

- Theorem 1:
  An integer n is prime if
  $(x+1)^n \equiv x^n + 1\ (mod\ n)\ in\ \mathbb{Z}[x]$
- **<u>Main theorem:</u>**
- For given integer $n \geq 2,$ let r be a positive integer $< n$, for which n has order $> (\log(n))^2 \quad (mod\ r)$.
  Then n is prime if and only if
  - n is not a perfect power
  - n does not have a prime factor $\leq r$
  - $(x+a)^n \equiv x^n + a$ $\big(mod(n,\ x^r - 1)\big)\ in\ \mathbb{Z}[x]$ for each integer a with $1 \leq a \leq \sqrt{r}\log(n)$

Algorithm

- Input: integer n
- Output: "n is prime" or "n in composite"

1. Determine whether n is perfect power
2. Find integer r with $ord(n)\ mod\ r\ > \log(n)^2$
3. Compute $n^j\ (mod\ q)$ for $j = 1, \dots, \lceil \log(n)^2 \rceil$ and each integer $q > \lfloor \log(n)^2 \rfloor$ until find q for which non of $n^j\ \equiv 1(mod\ q)$
4. Take $r = q$
5. Determine whether $gcd\ (a,n) > 1$ for an $a \leq r$
6. Determine whether $(x+a)^n \equiv x^n + a$
   for $a = 1,2, \dots, \lceil \sqrt{r}\log(n) \rceil$