16.06.2017

RWTH AACHEN UNIVERSITY

6.2. (Fermat's little theorem)

If p prime, $(a,p)=1$, then

$$a^{p-1} \equiv 1 \pmod{p}$$ ⊥

6.1. Probabilistic Primality Testing

Call n composite, if n is not prime.

Question: Is n composite?

FPT – Fermat Primality Test

- Select randomly some $a \in \{2, \dots, n-1\}$.
- Compute $a^{n-1} \bmod n$.
- $a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ composite
- Otherwise declare "n prime".

It holds that

$$n \text{ composite}, a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^* \Rightarrow a^{n-1} \not\equiv 1 \pmod{n}$$

Proof. Suppose $a^{n-1} \equiv 1 \pmod{n}$

$\Rightarrow a^{-1}$ exists, namely $a^{-1} \equiv a^{n-2}$

$\Rightarrow \gcd(a,n) = 1 \Rightarrow a \in \mathbb{Z}_n^*$. □

The least favorable case for ~~proof~~ FPT is:

n composite and $a^{n-1} \equiv 1 \pmod n$ $\forall a \in \mathbb{Z}_n^*$

Such numbers are called Carmichael numbers.

The first ones are

561, 1105, 1729, 2465, 2821, 6601, 29341,
172081, 278545, ...

Proposition 6.3. Let n composite (odd), no Carmichael number. Then

$$\#\{a \in \mathbb{Z}_n \setminus \{0\} \mid a^{n-1} \not\equiv 1 \pmod n\} \geq (>) \frac{n}{2}.$$

Proof. (Ex)

Hence, for algorithm FPT, provided n is no Carm. no.

$P($ FPT states "n composite" $|$ n composite $) \geq \frac{1}{2}$

$P($ FPT states "n prime" $|$ n composite $) \leq \frac{1}{2}$

Moreover

$P($ FPT states "n prime" $|$ n prime $) = 1$

By repeating the FPT independently m times the error prob. will be less than $\frac{1}{2^m}$.

Now: Probabilistic primality test such that

n prime $\Rightarrow$ Test declares "n prime" with prob. 1

n composite $\Rightarrow$ Test declares "n composite" with prob $\geq \frac{3}{4}$

(no worries about Carmichael numbers)

Def. 6.4. Let $n = 1 + q2^k$, q odd. (easy to determine)
Let $a \in \mathbb{N}$, $2 \leq a \leq n-1$.
a is called a strong witness (to compositeness), if

(i) $a^q \not\equiv 1 \pmod n$

(ii) $a^{q \cdot 2^i} \not\equiv -1 \pmod n$, $i = 0, 1, \ldots, k-1$.

Abbr. $a \in W(n)$.

Prop. 6.5 $\exists\, a \in W(n) \Rightarrow n$ is composite.

Proof. Suppose $a \in W(n)$ and n prime. By Fermat

$$a^{n-1} = a^{q \cdot 2^k} \equiv 1 \pmod n$$

Consider successive squares

$$\underbrace{a^q}_{\not\equiv 1 \pmod n},\ a^{q \cdot 2},\ a^{q \cdot 2^2},\ a^{q \cdot 2^3},\ \ldots,\ \underbrace{a^{q \cdot 2^k}}_{\equiv 1 \pmod n}$$

Let $j = \max\{0 \leq i \leq k-1 \mid a^{q \cdot 2^i} \not\equiv 1 \pmod n,\ a^{q \cdot 2^{i+1}} \equiv 1 \pmod n\}$

$b = a^{q 2^j}$, such that $b \not\equiv 1 \pmod n$, $b^2 \equiv 1 \pmod n$

n prime $\Rightarrow \mathbb{Z}_n$ is a field $\Rightarrow b \equiv 1$ or $b \equiv -1 \pmod n$

In summary: $b \equiv -1 \pmod n$. Contradiction to (ii). ∎

There are only a few $a \in \{2, \dots, n-1\}$ with $a \notin W(n)$.

Theorem 6.6. (Rabin, 1980)

For any odd, composite $n \in \mathbb{N}$ it holds that

$$\#\{a \mid 2 \le a \le n-1,\ a \notin W(n)\} \le \frac{n}{4}. \quad \_1$$

Proof. N. Koblitz (1994), p. 130 ff. ∎

MRPT – Miller-Rabin Primality Test

Write $n = 1 + q2^k$, q odd
Choose $a \in \{2, \dots, n-1\}$ at random ($a \sim U(\{2, \dots, n-1\})$)
$y := a^q \bmod n$;
if $y = 1$ then (return "n prime"; stop)
for $i := 1$ to k do begin
    if $y = n-1$ then (return "n prime"; stop)
    $y = (y * y) \bmod n$
    end;
return "n composite".

Application: Repeat MRPT m times with independently chosen a's $\in \{2,\dots,n-1\}$.

If MRPT returns m times "n prime", decide "n prime", otherwise decide "n composite".

$$P(\text{decide "}n\text{ prime"} \mid n \text{ composite}) \leq \left(\frac{1}{4}\right)^m = \frac{1}{4^m}$$

$$P(\text{decide "}n\text{ prime"} \mid n \text{ prime}) = 1$$

Exponentially decreasing error bound:

$$\frac{1}{4^{10}} = 0.95 \cdot 10^{-6}, \quad \frac{1}{4^{20}} = 0.91 \cdot 10^{-12}$$

How to find large prime numbers:

Choose $n \in \mathbb{N}$ (n large). Iterate $n := n+1$ until a prime number n is found by the MRPT.

The prime number theorem states:

$$\#\{p \mid p \leq n, p \text{ prime}\} \sim \frac{n}{\ln n}$$

Hence, the prob. that a randomly chosen $m \leq n \in \mathbb{N}$ is prime is $\sim \frac{1}{\ln n}$.

Ex: $n = 2^{512}$, select odd integers: $\frac{2}{\ln 2^{512}} \approx \frac{1}{177.4}$.

Remark. August 2002 a polynomial time deterministic algorithm for determining "prime" was published. by

Agrawal, Kayal, Saxena

Annals of Math., 160, (2004), 781-793.

General assessment.

- There is a polynomial time algorithm
- Much slower than MRPT
- My personal feeling: we can live with an error prob. of 2^{-1000}, say.

6.2 The Integer Factorization Problem

"Easy": Decide whether a given $n \in \mathbb{N}$ is composite.

"Hard": Find its prime factorization