6. Number-Theoretic Reference Problems

Consider $\mathbb{Z}_n$: ring of equivalence classes modulo n within integers.

$s, t \in \mathbb{Z}$: $s \sim t$ or $s \equiv t \ (\mathrm{mod}\ n)$

$\Leftrightarrow \quad n \mid (s-t)$

($\sim$ forms an equivalence relation over $\mathbb{Z}$)

$(\mathbb{Z}_n, +, \cdot)$ forms a ring

$(\mathbb{Z}_n, +)$ Abelian group

$(\mathbb{Z}_n, \cdot)$ associativ, 1 exists

& distributive law

<u>Def. 6.1</u> $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}$

is called the <u>multiplicative group</u> of $\mathbb{Z}_n$.

$\varphi(n) = \underbrace{|\mathbb{Z}_n^*|}_{\text{(order / cardinality of } \mathbb{Z}_n^*)}$ is called the Euler-φ-function.

Remarks:
- $\varphi(p) = p-1$, if p prime.
- $\mathbb{Z}_n^*$ is a multiplicative Abelian group. It holds $\gcd(a,n) = 1 \Leftrightarrow \exists$ inverse s of a, i.e., $a \cdot s \equiv s \cdot a \equiv 1$, $(\mathrm{mod}\ n)$
- Notation $\gcd(a,n) = (a,n)$. If $(a,n) = 1$, a and n are called <u>relatively prime</u> or <u>coprime</u>.

Th. 6.2. (Euler, Fermat)

If $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \pmod n$

In particular (Fermat's little theorem)

If p prime, $(a,p)=1$, then $a^{p-1} \equiv 1 \pmod p$. $\perp$

6.1. Probabilistic Primality Testing

Given $n \in \mathbb{N}$ (call n composite, if n is not prime)

Question: Is n composite?

FPT – Fermat Primality Test

Select randomly some $a \in \{2, \dots, n-1\}$.

$a^{n-1} \not\equiv 1 \pmod n \Rightarrow n$ composite

Otherwise declare 'n prime'

It holds that

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

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

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

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

The least favorable case is:

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

Such numbers are called <u>Carmichael numbers</u>

The first ones are

561, 1105, 1729, 2465, ..., 172 081, 278 545, ...

<u>Proposition 6.3.</u> Let n be composite (odd), no Carmichael no. Then

$$\left|\{a \in \mathbb{Z}_n \setminus \{0\} \mid a^{n-1} \not\equiv 1 \pmod n\}\right| \geq \overset{(>)}{\frac{n}{2}}. \quad \lrcorner$$

Hence, for alg. FPT, provided n is no Carmichael no:

$P($FPT states "n composite" $\mid n$ composite$) \geq 1/2$ or equ.

$P($FPT states "n prime" $\mid n$ composite$) \leq 1/2$.

Moreover

$P($FPT states "n prime" $\mid n$ prime$) = 1$.

Advantage: Very simple, fast

error prob. $\leq \frac{1}{2^M}$, if it is independently repeated M times, provided n is no Carm. no.

Aim: 1. n prime $\Rightarrow$ alg. declares "n prime" with prob. 1

2. n composite $\Rightarrow$ alg. declares "n comp." with prob. $\geq \frac{3}{4}$.

<u>Def. 6.4.</u> Let $n = 1 + q \cdot 2^k$, q odd.

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

$(\Leftrightarrow a^{q \cdot 2^i} \not\equiv n-1 \pmod n)$

Abbr. $a \in W(n)$. ⊥

<u>Prop. 6.5.</u> $\exists a \in W(n) \Rightarrow n$ is composite.

<u>Proof.</u> Suppose $a \in W(n)$ and n prime. By Fermat

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

Consider successive squares

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

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 $b \not\equiv 1 \pmod n$ and $b^2 \equiv 1 \pmod n$

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

Hence: $b \equiv -1 \pmod n$. Contradiction to (ii). ☒

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

<u>Theorem 6.6.</u> (Rabin, 1980)

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

$$|\{a \mid 2 \leq a \leq n-1,\ a \notin W(n)\}| \leq \frac{n}{4}.$$

[Proof. Rabin (1980), N. Koblitz]

Hence, choosing $a \in \{2,...,n-1\}$ at random with $a \notin W(n)$ has prob. $\leq \frac{1}{4}$.

MRPT – Miller-Rabin Primality Test

```
Write n = 1 + q·2^k , q odd
Choose a ∈ {2,...,n-1} at random (a ~ U({2,...,n-1}))
y := a^q mod 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) mod n
    end;
return "n composite"
```

Apply MRPT M times independently.

$$P(\text{decide "}n\text{ prime"} \mid n \text{ composite}) \le \frac{1}{4^k}$$

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

Exponentially decreasing error bound:

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

Remark:

Since 2002 there is a polynomial time deterministic primality test.

M. Agrawal, N. Kayal, N. Saxena: PRIMES is in $\mathcal{P}$.

How to find large primes?

Choose $n \in \mathbb{N}$ (large, odd)? ~~Iterate~~ $n := n + 2$ until a prime number is found by MRPT.

The prime number theorem states:

$$|\{p \mid p \le n, p \text{ prime}\}| \sim \frac{n}{\ln n}$$

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

Ex: $n = 2^{512}$, select only odd integers:

$$\frac{2}{\ln 2^{512}} \approx \frac{1}{177.4}$$

RWTH AACHEN UNIVERSITY

6.2. The Integer Factorization Problem

"Easy": decide if n is comp. or prime.

"Hard": Find the prime factors.