Lecture 4 (part 3) — Witnesses (svedkovia)

> Course **2-INF-135/15 Pravdepodobnostné algoritmy**, LS 2025/26. Source slides: `04_metody456.pdf`, slides 20–45 (the **witness** method). Part 1 was *eliminating the adversary*; part 2 was *fingerprints*. This is the **fourth method — witnesses**, and its two big customers: **primality testing** and **all-pairs shortest paths via fast matrix multiplication**.

Where we are: the fourth method

The catalogue from part 1 listed six design methods. We have done *eliminating the adversary* (online problems) and *fingerprints* (Freivalds, hashing, matching). Now:

> **Witnesses (svedkovia).** To decide whether an object has a property, *randomly hunt for a witness* — a small certificate that, if found, **proves** the property, and whose validity is **easy to check**.

The whole method lives or dies on one number: **how dense are the witnesses?** If a constant fraction of candidates are witnesses, random sampling finds one fast. The mathematical work in this lecture is almost entirely *proving that witnesses are dense* — and the recurring tool for that is **Lagrange's theorem** (a proper subgroup has at most half the elements).

---

1. The witness method, abstractly

We have a universe of **candidates** and want to test object O for a property P. A **witness** is a candidate a such that the pair (O, a) carries an *efficiently checkable proof* that O has property P.

Three requirements turn this into an algorithm (slides 21, 24):

1. **Easy to verify** a candidate: given a, deciding "is a a witness for O?" is efficient.
2. **Witnesses are dense**: the ratio (candidates : witnesses) is a *constant* — so a random candidate is a witness with constant probability.
3. **Efficient access** to candidates: we can sample one uniformly at random.

The algorithm is then trivial:

> Pick a candidate a at random. Check if it is a witness.

- **Witness found** → report "O has property P" — *this is certain*.
- **No witness** → report "O probably does **not** have P."

> **Punchline — this is exactly the co-RP / one-sided-error shape from Lecture 3.** A found witness is *gospel* (no false positives). The only error is *failing to find* a witness that exists — a false negative. Repeat with r fresh candidates: if witnesses have density $\geq \frac{1}{2}$, the chance of missing one r times is $\leq 2^{-r}$. Amplification is free.

For primality the property will be "n **is composite**", and a witness for n being composite is what the next sections build, step by step, fixing each failed attempt.

---

2. The number-theory toolbox (slide 22)

Everything below runs on four classical facts. Keep them on a card.

Little Fermat (malá Fermátová veta). If p is prime and $a \in \mathbb{Z}_p^* = \{d : \gcd(d,p) = 1\}$, then $a^{p-1} \equiv 1 \pmod{p}$.

Chinese Remainder Theorem, version I. If $m = m_1 \cdots m_k$ with the m_i pairwise coprime, then any tuple of residues $(r_1, \ldots, r_k)$ corresponds to a **unique** $r \in \mathbb{Z}_m$ with $r \equiv r_i \pmod{m_i}$.

Chinese Remainder Theorem, version II (the one we actually use). If $n = p \cdot q$ with $\gcd(p,q) = 1$, then the ring $\mathbb{Z}_n$ is **isomorphic** to $\mathbb{Z}_p \times \mathbb{Z}_q$: $a \longleftrightarrow (a \bmod p,\ a \bmod q)$, and addition/multiplication act coordinatewise. *Reading a number by its two "coordinates" mod p and mod q is how we will construct witnesses by hand.*

Lagrange's theorem. For a subgroup H of a finite group A, $|A| = \mathrm{Index}_H(A) \cdot |H|$, so $|H|$ **divides** $|A|$. In particular a *proper* subgroup has index ≥ 2, hence $|H| \leq |A|/2$.

> **Why Lagrange is the hero of this lecture.** Almost every "witnesses are dense" theorem has the same skeleton: the **non-witnesses form a proper subgroup** of $\mathbb{Z}_n^*$. By Lagrange that subgroup has $\leq |\mathbb{Z}_n^*|/2$ elements, so **at least half** the group are witnesses. Density $\geq \frac{1}{2}$ falls out of group theory, not of any delicate counting.

---

3. Attempt 0 — the divisor witness (and why it fails)

The naive definition: n is prime iff its only divisors are 1 and n. So a **divisor** $a \mid n$ with $1 < a < n$ is a perfectly valid witness that n is composite — and trivially checkable.

The problem is **requirement 2 (density)**. Take the hardest composites, $n = p \cdot q$ with $p, q \approx \sqrt{n}$ (RSA-shaped numbers). Among the $n - 1$ candidates there are only a *handful* of divisors. The witness density is $\approx 1/\sqrt{n}$, astronomically far from constant. Random sampling would never hit one.

> **Lesson.** Divisors prove compositeness but are far too rare. We need a *different, denser* notion of witness for the same property. The rest of §4–§9 is the search for one.

---

4. Attempt 1 — the Fermat witness (and the Carmichael catastrophe)

Little Fermat says: if n is prime, then $a^{n-1} \equiv 1 \pmod{n}$ for **every** $a \in \mathbb{Z}_n^*$. Contrapositive:

> a is a **Fermat witness** for "n composite" if $a^{n-1} \bmod n \neq 1$.

If we ever see $a^{n-1} \not\equiv 1$, then n *cannot* be prime — certain proof.

It is efficient to test (iterated squaring / opakované umocňovanie). We never form a^{n-1} as an integer; we reduce mod n after every squaring:
$a^2 \bmod n, \quad a^{2^k} \bmod n = \left[(a^{2^{k-1}} \bmod n)^2\right] \bmod n,$ and for $n - 1 = \sum_i b_i 2^{i-1}$ we multiply together the $a^{2^{i-1}}$ with $b_i = 1$. That is $O(\log n)$ multiplications in $\mathbb{Z}_n$, i.e. $O((\log n)^3)$ **bit operations**. Cheap.

The catastrophe: Carmichael numbers (Carmichaelove čísla). There exist *composite* n for which $a^{n-1} \equiv 1 \pmod{n}$ **for all** a **coprime to** n**.** The smallest is $561 = 3 \cdot 11 \cdot 17$. For such n the Fermat test has **no witnesses at all** among coprime a — density 0, requirement 2 dead. (There are infinitely many Carmichael numbers, so this is not a finite annoyance we can table.)

> **Punchline.** Fermat's test is fast and one-sided but *not robust*: Carmichael numbers are composites that the test cannot distinguish from primes. We need a witness that survives even them. Two routes do it: looking at **square roots of** 1 (Miller–Rabin, §6) and the **Jacobi symbol** (Solovay–Strassen, §7).

5. The fix's foundation — an algebraic characterization of primes (slides 25–26)

The escape is to test not a^{n-1} but its **square root** $a^{(n-1)/2}$.

Theorem (alternative definition of a prime). For odd $p > 2$,
$p \text{ is prime} \iff a^{(p-1)/2} \bmod p \in \{1,\, p-1\} \ \ \forall a \in \mathbb{Z}_p \setminus \{0\}.$

Proof sketch.

- **($\Rightarrow$)** Write $p = 2p' + 1$. By Fermat $a^{p-1} - 1 \equiv 0$, and over the **field** $\mathbb{Z}_p$ we may factor $a^{p-1} - 1 = \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p}$. A field has no zero divisors, so one factor vanishes: $a^{(p-1)/2} \equiv \pm 1$, i.e. $\in \{1, p-1\}$.
- **($\Leftarrow$)** Suppose the property holds for all $x \neq 0$ but $p = ab$ were a proper factorization. Then $0 \equiv p \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \in \{1, -1\} \pmod{p}$ — contradiction, since $0 \notin \{1, -1\}$ mod p. $\square$

The number $a^{(n-1)/2}$ is a square root of a^{n-1}. For a prime it must be one of the **trivial** roots of unity ± 1. Composites can have *other* roots — and those other roots are the new, denser witnesses.

---

6. The clean case $n \equiv 3 \pmod 4$ — and the density engine (slides 25, 27, 28)

For the special shape $n \equiv 3 \pmod 4$ the witness is simply: $a^{(n-1)/2}$ landing *outside* $\{1, n-1\}$.

Theorem. For $n \equiv 3 \pmod 4$:

- if n is **prime**, then $a^{(n-1)/2} \bmod n \in \{1, n-1\}$ for all a;
- if n is **composite**, then $a^{(n-1)/2} \bmod n \notin \{1, n-1\}$ for **more than half** of $a \in \{1, \ldots, n-1\}$.

So define the witness set and its complement (the "liars"):
$\mathbf{Wit} = \{a : a^{(n-1)/2} \bmod n \notin \{1, n-1\}\}, \qquad \mathbf{Euler} = \{a : a^{(n-1)/2} \bmod n \in \{1, n-1\}\}.$

Why $|\mathbf{Wit}| \geq |\mathbf{Euler}|$ — the injection argument. This is the heart, and it is beautiful. Suppose we have **one** witness $b \in \mathbf{Wit}$ (we construct one below). Define
$h_b : \mathbf{Euler} \to \mathbf{Wit}, \qquad h_b(a) = a \cdot b \bmod n.$

- **It lands in Wit.** Since $a \in \mathbf{Euler}$, $a^{(n-1)/2} \equiv \pm 1$, so $(ab)^{(n-1)/2} = a^{(n-1)/2}\, b^{(n-1)/2} = (\pm 1)\, b^{(n-1)/2}$. As $b^{(n-1)/2} \notin \{1, -1\}$, multiplying by ± 1 keeps it outside $\{1, -1\}$. Hence $h_b(a) \in \mathbf{Wit}$. ✓

- **It is injective.** If $a_1 b \equiv a_2 b \pmod{n}$, multiply by b^{-1} (exists because $b \in \mathbb{Z}_n^*$): $a_1 \equiv a_2$. ✓

An injection $\mathbf{Euler} \hookrightarrow \mathbf{Wit}$ gives $|\mathbf{Euler}| \leq |\mathbf{Wit}|$, so witnesses are **at least half** of $\mathbf{Euler} \cup \mathbf{Wit}$.

> **This is the Lagrange idea in disguise.** Multiplying by a fixed b is a "coset shift": it maps the liars injectively onto (part of) the witnesses, so the liars can be at most half. One real witness ⇒ a flood of them.

Constructing one witness b (slide 28). Let $n = p \cdot q$ with $\gcd(p, q) = 1$. By CRT II read every a as a pair $(a \bmod p,\ a \bmod q)$. Members of $\mathbf{Euler}$ map to $(1, 1)$ or $(p-1, q-1) = (-1, -1)$. Now *define* b by its coordinates $b \longleftrightarrow (1,\ q-1) = (1, -1)$. Then $b^{(n-1)/2} \leftrightarrow (1^{(n-1)/2}, (-1)^{(n-1)/2}) = (1, -1)$, which is **neither** $(1, 1)$ nor $(-1, -1)$ — so $b \notin \mathbf{Euler}$, i.e. $b \in \mathbf{Wit}$. (Bonus: b is its own inverse, since $(1, -1) \odot (1, -1) = (1, 1)$.) The witness exists; the injection fires; density $\geq \frac{1}{2}$. □

The catch: this only covers $n \equiv 3 \pmod{4}$. The two real algorithms remove that restriction.

---

7. Miller–Rabin — square roots of unity for *all* n (slide 23)

Miller–Rabin upgrades the Fermat test with one extra idea: **a nontrivial square root of 1 betrays a composite.** In a field, the only solutions of $x^2 \equiv 1$ are $x \equiv \pm 1$. So if we ever find x with $x^2 \equiv 1 \pmod{b}$ but $x \not\equiv \pm 1$, then b is **not** a field, hence not prime.

Write $b - 1 = 2^t \cdot (\text{odd})$, i.e. $2^t \mid (b-1)$ and $2^{t+1} \nmid (b-1)$. The chain of repeated square roots is $a^{(b-1)/2},\ a^{(b-1)/4},\ \ldots,\ a^{(b-1)/2^t}$.

> **Miller–Rabin test.** Input: odd $b > 2$, rounds r.
>
> 1. Find t with $2^t \,\|\, (b-1)$.
> 2. Repeat r times:
> 3. pick $a \in \{1, \ldots, b-1\}$ at random;
> 4. if some $x \in \{a^{(b-1)/2}, \ldots, a^{(b-1)/2^t}\}$ has $x^2 \equiv 1$ and $x \not\equiv \pm 1 \pmod{b}$ → **return "b is composite"** *(nontrivial root of 1)*;
> 5. if $a^{b-1} \not\equiv 1 \pmod{b}$ → **return "b is composite"** *(Fermat witness)*;
> 6. **return "b is probably prime."**

It catches both failure modes — Fermat witnesses *and* nontrivial square roots — and the second kind even nails **Carmichael numbers**, which the pure Fermat test missed.

Guarantee. If b is composite, then $\Pr_a[\,a \text{ is a witness}\,] \geq \frac{1}{2}$, so r independent rounds give error $\leq (1/2)^r$.

Cost. $O(r\,m^3)$ for an m-bit b. For $m = 340$ (≈ 100 decimal digits) and $r = 50$: $rm^3 \approx 2 \cdot 10^9$ operations, error $2^{-50} \approx 10^{-15}$. This is the primality test used in practice.

---

8. Solovay–Strassen — the Jacobi symbol for *all* n (slides 29–34)

A second route to a witness for all odd n, historically first, built on **quadratic residues**.

Legendre symbol (for prime p, $\gcd(a,p) = 1$):
$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a quadratic residue mod } p, \\ -1 & a \text{ is a non-residue.} \end{cases} \qquad \text{Euler:} \quad \left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Jacobi symbol (for odd $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$, $\gcd(a,n) = 1$):
$$\left(\frac{a}{n}\right) = \prod_{i=1}^{\ell} \left(\frac{a}{p_i}\right)^{k_i} = \prod_{i=1}^{\ell} \left(a^{(p_i-1)/2} \bmod p_i\right)^{k_i}.$$

> **The crucial efficiency fact.** The Jacobi symbol can be computed **without factoring** n — by reciprocity rules (slide 30) that look exactly like a Euclidean GCD: each step at least halves a parameter, so depth $O(\log n)$ and total $O((\log n)^3)$ bit operations. The rules are
> $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ if $a \equiv b$, $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$, $\left(\frac{n}{a}\right)\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}$.

Solovay–Strassen witness. a is a witness for "n composite" if either
$$\gcd(a,n) \neq 1, \qquad \text{or} \qquad \gcd(a,n) = 1 \text{ and } \left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n.$$

Theorem. For odd $n \geq 3$:

- if n is **prime**, then $\left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n$ for *every* a (this is exactly Euler's criterion);
- if n is **composite**, then $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n$ for at least **half** the a with $\gcd(a,n) = 1$.

The density proof is the Lagrange/subgroup argument again. Let the non-witnesses be $\overline{\text{Wit}}_n = \left\{a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n\right\}$. This set is **closed under multiplication** (slide 32): if a, b each satisfy it then $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = a^{(n-1)/2} b^{(n-1)/2} = (ab)^{(n-1)/2} \pmod n$, so $ab \in \overline{\text{Wit}}_n$ — it is a **subgroup** of $\mathbb{Z}_n^*$. To finish we must show it is a **proper** subgroup, i.e. exhibit some $a \in \mathbb{Z}_n^*$ *outside* it (slides 32–34). With $n = p_1^{i_1} m$, two cases:

- **$i_1 = 1$ (p_1 appears to the first power).** Let g generate the cyclic group $\mathbb{Z}_{p_1}^*$ and use CRT to set $a \equiv g \pmod{p_1}$, $a \equiv 1 \pmod{m}$. A generator is a non-residue, so $\left(\frac{a}{n}\right) = -1$, while $a^{(n-1)/2} \equiv 1$ — they differ, so a is a witness.

- $i_1 \geq 2$ **(a square factor).** If $a \in \overline{\mathbf{Wit}_n}$ then $a^{n-1} \equiv 1$, forcing the order $|\mathbb{Z}_q^*|$ (with $q = p_1^{i_1}$) to divide $n-1$. But $p_1 \mid |\mathbb{Z}_q^*|$ and $p_1 \mid n$, so $p_1 \mid \gcd(n, n-1) = 1$ — contradiction. A witness must exist.

By Lagrange the proper subgroup has $\leq |\mathbb{Z}_n^*|/2$ elements, so witnesses are $\geq$ half. □

> **Algorithm SSA (Solovay–Strassen), input odd $n \geq 3$:** pick random $a \in \{1, \ldots, n-1\}$; if $\gcd(a, n) \neq 1$ return *composite*; else compute $J = \left(\frac{a}{n}\right)$ and $A = a^{(n-1)/2} \bmod n$; return *prime* if $J = A$, else *composite*. Everything is $O((\log n)^3)$.

---

9. From testing to *generating* primes (slides 35–37)

Cryptography needs random primes. `PrimGen(ℓ, k)`: repeatedly draw a random odd ℓ-bit number $n = 2^{\ell-1} + \sum_{i=1}^{\ell-2} a_i 2^i + 1$ and run k rounds of Solovay–Strassen; output the first n that passes. There are two error sources, and both are crushed.

Error A — fails to output any prime. By the Prime Number Theorem a random ℓ-bit number is prime with probability $\geq \frac{1}{\ln n} > \frac{1}{2\ell}$. Over $2\ell^2$ attempts, $\Pr[\text{no prime found and certified}] < \left(1 - \frac{1}{2\ell}\right)^{2\ell^2} \cdot (\text{test-miss factor}) < e^{-\ell}$. For $\ell \geq 100$: $e^{-100} \ll 10^{-40}$.

Error B — outputs a composite as "prime". Each run lets a composite slip with probability $\leq 2^{-\ell}$ (with $k = \ell$ rounds). Summed over the $\leq 2\ell^2$ attempts, $\Pr[\text{output composite}] \leq \frac{\ell^2}{2^{\ell-1}}$. For $\ell \geq 100$: $\leq 1.58 \cdot 10^{-26}$.

> **Punchline.** A *Monte-Carlo* test (one-sided error on a single number) composes into a *generator* whose two failure modes are both exponentially unlikely. You get a prime with overwhelming confidence and no factorization in sight — the bedrock of RSA key generation.

---

10. The second arena — witnesses for a Boolean matrix product (slides 38–45)

The witness method is **not** only number theory. Its second appearance is a gem of algorithm design: **all-pairs shortest paths (APSP)** in an *unweighted, undirected* graph, via fast matrix multiplication. Let $\mathrm{MM}(n) = n^\omega$ be the cost of multiplying two $n \times n$ matrices.

	distances only	**distances and paths**
deterministic	BFS $O(mn)$, Floyd–Warshall $O(n^3)$	—
randomized	APD $O(\mathrm{MM}(n)\log n)$	+ BPWM $\rightarrow O(\mathrm{MM}(n)\log^2 n)$

10a. APD — distances by halving (Seidel), slides 39–40

Build G' by adding an edge between any two vertices at distance ≤ 2 in G (computed from A and A^2: $Z = A^2$, then $B[i,j] = A[i,j] \vee Z[i,j]$). Distances in G' are *halved*:
$D[i,j]$ even $\Rightarrow D[i,j] = 2D'[i,j]$, $\quad$ $D[i,j]$ odd $\Rightarrow D[i,j] = 2D'[i,j] - 1$. Recurse on G' to get D', then recover the parity of $D[i,j]$ from a neighbour sum (slide 39): $D[i,j]$ is even
$\iff \sum_{k\in\Gamma(i)} D'[k,j] \;\ge\; \deg(i)\, D'[i,j]$. The recursion
$T(n,\delta) = 2\,\mathrm{MM}(n) + T(n, \lceil \delta/2 \rceil) + O(n^2)$ gives
$\boxed{\text{APD computes the full distance matrix in } O(\mathrm{MM}(n)\log n).}$

But distances are **not** paths. To walk a shortest i–j path we need, at i, *some neighbour k on a shortest path to j*. Finding that k is a **witness** problem.

10b. APSP reduces to BPWM (slide 41–42)

Define the **Boolean Product Witness Matrix** problem:

> **BPWM.** Given Boolean matrices A, B, output W where $W[i,j] = k$ for *some* k with $A[i,k] = B[k,j] = 1$ (a **witness** for the Boolean product entry), or 0 if none exists.

A successor on a shortest path is exactly such a witness: $S[i,j] = k$ iff $A[i,k] = 1$ (k is a neighbour of i) and $D[k,j] = D[i,j] - 1$. We don't want to solve this for all $n-1$ possible distance values — but neighbours satisfy $D[i,j] - 1 \le D[k,j] \le D[i,j] + 1$, so it suffices to match $D[k,j] \equiv D[i,j] - 1 \pmod 3$. Run BPWM on A against the three "distance-class" matrices $D^{(r)}$ ($r \in \{0,1,2\}$). **Three** products replace $n-1$.

10c. Finding the witness — isolate it by subsampling (slides 43–45)

How do we extract an actual witness k from a Boolean product? Two ideas.

Idea 1: a unique witness reveals itself arithmetically. Compute the *integer* product $W = A \cdot B$. Then $W[i,j]$ **counts** the witnesses k. Now weight column k of A by the number k and multiply: the (i,j) entry becomes $\sum_k k\,A[i,k]B[k,j]$ = *sum of all witness indices*. **If there is exactly one witness k^*, this sum equals k^*** — the witness drops out for free.

Idea 2: make "exactly one" happen, by random subsampling. When (i, j) has c witnesses, randomly keep a subset of d columns $k_1, \ldots, k_d$. If we pick the *scale* d so that $n/2 \le c\,d \le n$, exactly one witness survives with good probability:

> **Balls lemma.** Among n balls, w are white. Draw d independently with replacement, with $n/2 \le wd \le n$. Then $\Pr[\text{exactly one white}] = d\,\frac{w}{n}\left(1-\frac{w}{n}\right)^{d-1} \ge \frac{1}{2}\left(1-\frac{1}{d}\right)^{d-1} > \frac{1}{2e}$.

Proof. $d \cdot \frac{w}{n} \ge \frac{1}{2}$ from $wd \ge n/2$; and $\frac{w}{n} \le \frac{1}{d}$ from $wd \le n$, so $(1-\frac{w}{n})^{d-1} \ge (1-\frac{1}{d})^{d-1} > e^{-1}$. □

Since c is unknown, try every scale $d = 2^\ell$ for $\ell = 0, \ldots, \lceil \log n \rceil - 1$, each repeated $3.42\lceil \log n \rceil$ times. For the right scale a single try isolates a witness with probability $\ge \frac{1}{2e}$, so the chance of *never* isolating one is $\left(1-\frac{1}{2e}\right)^{3.42\lceil \log n \rceil} \le \frac{1}{n}$. Hence only a $\le 1/n$ fraction of entries fall through to a direct computation (step 3), and the whole witness matrix costs $O(\mathrm{MM}(n)\log^2 n)$.

> **Punchline.** This is the *same* deep idea as the Isolation Lemma from part 2: when many solutions confuse you, **randomly thin them down until exactly one survives** — a *unique* witness is one you can read off arithmetically. Randomness here is not for speed but for **isolation**.

Recurring themes from the witness method

Theme	Where it appeared
One found witness = certain proof (co-RP / one-sided error)	every primality test (§1)
Density of witnesses is everything	divisor fails (§3), Fermat fails on Carmichael (§4)
Non-witnesses form a (proper) subgroup → Lagrange → ≤ half	$n \equiv 3 \bmod 4$ (§6), Solovay–Strassen (§8)
One witness floods into many (multiply by b: injective coset shift)	injection $\mathbf{Euler} \hookrightarrow \mathbf{Wit}$ (§6)
Read a number by CRT coordinates $(\bmod p, \bmod q)$	building an explicit witness b (§6, §8)
A nontrivial square root of 1 betrays a composite	Miller–Rabin (§7)
Compute a hard invariant without the hard data	Jacobi symbol *without factoring* (§8)
Monte-Carlo test → reliable generator	random prime generation (§9)
Isolate a unique witness by random subsampling	BPWM for shortest paths (§10)

The one sentence tying it together:

> **A witness is a needle whose mere existence is a proof — so the only question is how much hay surrounds it.** Group theory (Lagrange) guarantees the needles are at least half the haystack for primality; random subsampling *manufactures* a lone needle for matrix products. Find one and you are certain; the randomness only governs how fast you find it.