COMP 8920: Cryptography Winter 2025

Lecture 20 — Mar 20, 2025

Prof. Curtis Bright *Scribe: Aaron Barnoff*

1 Euler's Criterion

Let p be an odd prime. Then for any $a \in \mathbb{Z}_p$, the element a is a quadratic residue (QR) modulo p if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Proof

($\Rightarrow$) Suppose that there exists y such that

$$y^2 \equiv a \pmod{p}.$$

Raising both sides to the power $\frac{p-1}{2}$ gives

$$\left(y^2\right)^{\frac{p-1}{2}} \equiv y^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem, we have $y^{p-1} \equiv 1 \pmod{p}$; hence,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

($\Leftarrow$) Conversely, suppose that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Let b be a primitive root (generator) of $\mathbb{Z}_p^*$ so that every nonzero element modulo p can be written as a power of b. Then there exists some positive integer i for which

$$b^i \equiv a \pmod{p}.$$

It follows that

$$a^{\frac{p-1}{2}} \equiv \left(b^i\right)^{\frac{p-1}{2}} = b^{\frac{i(p-1)}{2}} \equiv 1 \pmod{p}.$$

Since the order of b is the order $\mathbb{Z}_p^* = p-1$, we deduce that $\frac{i(p-1)}{2}$ is a multiple of $p-1$, so $\frac{i}{2}$ must be an integer. Hence, i is even, say $i = 2k$. Then

$$a \equiv b^{2k} \pmod{p},$$

so that $\pm b^k$ are square roots of a modulo p. Thus, a is a quadratic residue. □

To check whether $a \pmod{p}$ is a quadratic residue, one can compute

$$a^{\frac{p-1}{2}} \pmod{p}$$

and verify that the result is 1. This computation requires $O(\log(p))$ multiplications of numbers having $O(\log p)$ bits each, costing a total of

$$O((\log p)^3)$$

bit operations.

Euler's criterion can also be stated in the following convenient form:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

where $\left(\frac{a}{p}\right)$ is the *Legendre symbol* defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Generalization: The Jacobi Symbol

For any odd positive integer n, with prime factorization

$$n = \prod_{i=1}^{k} p_i^{e_i},$$

the *Jacobi symbol* is defined by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Example: Consider

$$9975 = 3 \cdot 5^2 \cdot 7 \cdot 19.$$

Then,

$$\left(\frac{2}{9975}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right)^2 \cdot \left(\frac{2}{7}\right) \cdot \left(\frac{2}{19}\right)$$

Using Euler's criterion to compute the individual Legendre symbols, we have:

$$\begin{aligned} \left(\frac{2}{9975}\right) &= \left(2^{\frac{3-1}{2}} \pmod{3}\right) \cdot \left(2^{\frac{5-1}{2}} \pmod{5}\right)^2 \cdot \left(2^{\frac{2-1}{2}} \pmod{7}\right) \cdot \left(2^{\frac{19-1}{2}} \pmod{19}\right) \\ &= (-1) \cdot (-1)^2 \cdot 1 \cdot (-1) \\ &= 1. \end{aligned}$$

Note: The fact that $\left(\frac{a}{p}\right) = 1$ for an odd prime p implies that the congruence

$$y^2 \equiv a \pmod{p}$$

has a solution (for odd prime p); however, when n is composite the Jacobi symbol does not guarantee the existence of such a solution.

The Jacobi symbol is especially useful in primality testing. In many cases for a composite n, one finds that

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}.$$

For example, one may observe that

$$2^{\frac{9975-1}{2}} \equiv 9578 \pmod{9975},$$

which does not equal the Legendre symbol $\left(\frac{2}{9975}\right) = 1$, thereby indicating that Euler's criterion can fail for composite moduli.

Similarly, consider $n = 91$ (n is composite) and $a = 10$:

Then, the Jacobi symbol is $\left(\frac{10}{91}\right)$, and using the Jacobi symbol properties:

$$\left(\frac{10}{91}\right) = \left(\frac{10}{7}\right) \cdot \left(\frac{10}{13}\right).$$

Using quadratic reciprocity, we compute:

$$\left(\frac{10}{7}\right) = -1, \quad \left(\frac{10}{13}\right) = 1,$$

so

$$\left(\frac{10}{91}\right) = (-1) \cdot 1 = -1.$$

Now, computing $10^{\frac{91-1}{2}} \pmod{91}$ gives:

$$10^{\frac{91-1}{2}} \equiv 10^{45} \equiv -1 \pmod{91}.$$

Thus, we see that:

$$10^{\frac{91-1}{2}} \equiv \left(\frac{10}{91}\right) \pmod{91}.$$

Since this satisfies Euler's criterion, it suggests that 91 could be prime, even though we know it is composite. This situation is known as an *Euler pseudoprime* to base 10.

In fact, it can be shown that for a composite n, at least half of the choices $a \in \mathbb{Z}_n^*$ will expose the compositeness of n.

The Solovay-Strassen Primality Test

To gain confidence that a given odd integer n is prime, one may test many random choices of a using Euler's criterion. If n passes many trials, it is declared a *probable prime*. This forms the basis of the Solovay-Strassen algorithm.

Algorithm (Solovay-Strassen):

Input: An odd integer $n > 1$.

1. Select a random integer a from $\{2, 3, \ldots, n-1\}$.
2. If $\gcd(a, n) > 1$, then immediately return "composite".
3. Compute
$$y := a^{\frac{n-1}{2}} \pmod{n},$$
where y is represented in the symmetric range $\{-\frac{n-1}{2}, \ldots, \frac{n-1}{2}\}$.
4. If $y = \left(\frac{a}{n}\right)$, then return "probably prime" (here $\left(\frac{a}{n}\right)$ denotes the Jacobi symbol). Otherwise, return "composite".

Note: If n is prime, the algorithm always returns "probably prime."

Note: Since a is randomly selected, and at least half of $a \in \mathbb{Z}_p^*$ will reveal n to not be prime if n is composite, then each independent trial detects a composite n with probability at least 50%, so the error probability after m independent tests is at most $\left(\frac{1}{2}\right)^m$.

But how can we compute $\left(\frac{a}{n}\right)$ in the last step of the algorithm?

The Jacobi symbol defined above supposes we already know the prime factorization of n.

Computing the Jacobi Symbol $\left(\frac{a}{n}\right)$ Without Factorization

Even though the definition of the Jacobi symbol involves the prime factorization of n, it can be computed without factoring n by using the following properties for any odd positive integer n:

1. **Congruence Invariance:** If $m_1 \equiv m_2 \pmod{n}$, then
$$\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right).$$
2. **Evaluation for 2:**
$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$
3. **Multiplicativity:** For any integers m_1 and m_2,
$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right) \cdot \left(\frac{m_2}{n}\right).$$
In particular, if $a = 2^k \cdot t$, then
$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^k \cdot \left(\frac{t}{n}\right).$$
4. **Quadratic Reciprocity:** If m is odd, then
$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod{4}, \\ \left(\frac{n}{m}\right) & \text{otherwise.} \end{cases}$$

Property 3 can be used to "factor out" multiples of 2 from a. Property 2 can evaluate $\frac{2}{n}$. The remaining $\frac{t}{n}$ is handled with property 4, switching t and n, and $\frac{n}{t} = \frac{n \bmod t}{t}$ (given by property 1), which gives an expression with smaller numbers.

So, using these properties, one can recursively reduce the computation of $\left(\frac{a}{n}\right)$ to evaluations on smaller numbers. The process is similar to the Euclidean algorithm and requires $O(\log n)$ modular reductions on numbers of $O(\log n)$ bits, leading to an overall cost of

$$O((\log n)^3)$$

bit operations.

Error Probability Analysis via Bayes' Theorem

To use this to generate an RSA key, we select a large random integer a and test it m times with the Solovay-Strassen primality test algorithm. Assuming it passes all tests, what is the probability that n is prime?

Suppose we define:

- A: the event that a random odd integer n in the interval $[N, 2N]$ is composite.
- B: the event that the algorithm outputs "prime" in m independent trials.

Since a is always selected randomly, each independent trial detects compositeness with probability at least $1/2$, so we have

$$\mathbb{P}[B \mid A] \leq \left(\frac{1}{2}\right)^m.$$

However, we want $\mathbb{P}[A \mid B]$, the probability that a is composite given that the test passes m times. We get this from Baye's theorem and an estimate of $\mathbb{P}[A]$.

We get $\mathbb{P}[A]$ from the prime number theorem. The number of primes in $[N, 2N]$ is about $\frac{2N}{\ln(2N)} - \frac{N}{\ln(N)} \equiv \frac{n}{\ln(n)}$.

There are about $\frac{N}{2} \equiv \frac{n}{2}$ odd numbers in $[N, 2N]$, so

$$\mathbb{P}[\bar{A}] \equiv \frac{\frac{n}{\ln(n)}}{\frac{n}{2}} = \frac{2}{\ln(n)},$$

and so $\mathbb{P}[A] = 1 - \frac{2}{\ln(n)}$.

Also,

$$\begin{aligned}\mathbb{P}[b] &= \mathbb{P}[B \mid A] + \mathbb{P}[B \mid \bar{A}]\,\mathbb{P}[\bar{A}] \\ &\geq \mathbb{P}[B \mid \bar{A}]\,\mathbb{P}[\bar{A}] \\ &= 1 \cdot \frac{2}{\ln(n)},\end{aligned}$$

because for a prime n, the test never fails ($\mathbb{P}[B \mid \bar{A}] = 1$).

So,

$$\begin{aligned}\mathbb{P}[A \mid B] &= \frac{\mathbb{P}[B \mid A]\,\mathbb{P}[A]}{\mathbb{P}[B]} \\ &\leq 2^{-m} \cdot \frac{1 - \frac{2}{\ln(n)}}{\frac{2}{\ln(n)}} \\ &= 2^{-m} \cdot \frac{\ln(n) - 2}{2} \\ &= 2^{-(m+1)} \cdot (\ln(n) - 2).\end{aligned}$$

Hence, as m grows, the exponent gets small very quickly.

For instance, if n is a 1024-bit number ($n = 2^{1024}$, so $\ln n \approx 710$), then taking $m = 50$ trials yields

$$\mathbb{P}[A \mid B] \leq 2^{-51}(710 - 2),$$

an extremely small probability.

Further Refinements: The Miller-Rabin Test

In practice, composite numbers rarely pass even a single trial of such a test. Moreover, the Solovay-Strassen test can be improved upon by the Miller-Rabin test. The latter is based on the fact that a prime p has exactly two square roots of 1, namely ± 1. One can think of Euler's criterion

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \equiv \pm 1 \pmod{n}$$

as a "square root" version of Fermat's little theorem ($a^{n-1} \equiv 1 \pmod{n}$ for prime n).

If $a^{n-1} \equiv 1 \pmod{n}$ and $\frac{n-1}{2}$ is even, then one can take an additional square root to obtain

$$\frac{a^{n-1}}{4} \equiv \pm 1 \pmod{n}.$$

The Miller-Rabin test repeatedly takes square roots; if at any stage the square root is not ± 1, then n is composite.