Chapter 3

Primality Tests

A crucial question when implementing RSA is how to find the necessary primes for key generation. The answer will be given in form of efficient procedures. Start with a random integer of the desired length and test it for primality. If it is not prime take the next integer and so on. Eventually a prime will occur.

For this we need procedures that efficiently decide whether an integer is prime or not—primality tests.

We'll encounter a phenomenon that is familiar also with other mathematical problems (for instance linear optimization, numerical approximation of zeroes of polynomials over the real or complex numbers):

- There is an algorithm that gets by with polynomial cost.
- There is a "standard algorithm" (in the examples: the simplex method, the Newton algorithm) that is much more efficient for "most" instances, but needs more than polynomial cost in the "worst case". In practice this algorithm is the preferred one.

For primality testing the AKS algorithm is polynomial, but usually slower than the established Rabin algorithm. The latter is usually very efficient, but in the worst case even fails to deliver a correct result.

All these primality tests have a considerable overhead. Therefore for a practical implementation it makes sense to first check divisibility by "small" primes, say primes $< 10^6$, depending on the available storage (precompute a list L of small primes).

If we need a random prime of a certain size we randomly choose an integer r of this size. If r is even we increment it by 1. Then we sieve an interval $[r, r+s]$ for multiples of the primes in L by Eratosthenes' method. We test the remaining integers for primality until we find one that passes the test. In most cases this will be the first one already.

3.1 The Pseudoprime Test

How can we identify an integer as prime? The "naive" approach is trial divisions by all integers $\leq \sqrt{n}$, made perfect in the form of ERATOSTHENES sieve. An assessment of the cost shows that this approach is not efficient since $\sqrt{n} = \exp(\frac{1}{2} \log n)$ grows exponentially with the length $\log n$ of n.

An approach to identify primes without trial divisions is suggested by FERMAT's theorem: If n is prime, then $a^{n-1} \equiv 1 \pmod{n}$ for all $a = 1, \ldots, n-1$. Note that this is a necessary condition only, not a sufficient one. Thus we say that n is a (FERMAT) **pseudoprime to base** a if $a^{n-1} \equiv 1 \pmod{n}$. Hence a prime number is a pseudoprime to each base $a = 1, \ldots, n-1$.

Examples

1. The congruence $2^{14} \equiv 4 \pmod{15}$ shows that 15 is not prime.

2. We have $2^{340} \equiv 1 \pmod{341}$ although $341 = 11 \cdot 31$ is not prime. Anyway $3^{340} \equiv 56 \pmod{341}$, hence 341 fails the pseudoprime test to base 3.

The pseudoprime property is not sufficient for primality. Therefore we call n a CARMICHAEL **number** if n is a pseudoprime to each base a that is coprime with n, but n is not a prime.

Another way to express pseudoprimality is that the order of a in $\mathbb{M}_n$ divides $n-1$. Thus n is a CARMICHAEL number or prime if and only if $\lambda(n) \mid n-1$ with the CARMICHAEL function λ.

Unfortunately there are many CARMICHAEL numbers, so pseudoprimality cannot even considered as "almost sufficient" for primality. In 1992 ALFORD, GRANVILLE, and POMERANCE proved that there are infinitely many CARMICHAEL numbers.

The smallest CARMICHAEL number is $561 = 3 \cdot 11 \cdot 17$. This is a direct consequence of the next proposition.

Proposition 9 *A natural number n is a* CARMICHAEL *number if and only if it is not prime, squarefree, and $p-1 \mid n-1$ for each prime divisor p of n. An odd* CARMICHAEL *number has at least 3 prime factors.*

Proof. "$\Longrightarrow$": Let p be a prime divisor of n.

Assume $p^2|n$. Then $\mathbb{M}_n$ contains a subgroup isomorphic with $\mathbb{M}_{p^e}$ for some $e \geq 2$, hence by Proposition 18 in Appendix A.3 also a cyclic subgroup of order p. This leads to the contradiction $p \mid n-1$.

Since $\mathbb{M}_n$ contains a cyclic group of order $p-1$ it has an element a of order $p-1$, and $a^{n-1} \equiv 1 \pmod{n}$, hence $p-1 \mid n-1$.

"$\Longleftarrow$": Since n is squarefree by the chinese remainder theorem the multiplicative group $\mathbb{M}_n$ is the direct product of the cyclic groups $\mathbb{F}_p^\times$ where p runs through the prime divisors of n. Since all $p-1 \mid n-1$ the order of each element of $\mathbb{M}_n$ divides $n-1$.

Proof of the addendum: Let n be an odd CARMICHAEL number. Suppose $n = pq$ with two primes p and q, say $p < q$. Then $q-1 \mid n-1 = pq-1$, hence $p-1 \equiv pq-1 \equiv 0 \pmod{q-1}$. This contradicts $p < q$. $\diamond$

3.2 Strong Pseudoprimes

For a stronger pseudoprime test we use an additional characteristic property of primes.

Assume that n is odd, but not a prime nor a prime power. Then the residue class ring $\mathbb{Z}/n\mathbb{Z}$ contains non-trivial square roots of 1 besides ± 1. If we find one of these, then we have a proof that n is composite. But how to find non-trivial square roots of 1 when the prime decomposition of n is unknown?

Picking up an idea from Section 2.2 we decompose $n-1$ as

$$n - 1 = 2^s \cdot r \quad \text{with odd } r \tag{1}$$

(and call s the **2-order** of $n-1$). Let $a \in \mathbb{M}_n$. If n fails the pseudoprime test to base a, then it is identified as composite. Otherwise the order of a in the multiplicative group $\mathbb{M}_n$ divides $n-1$. Consider the sequence

$$a^r \bmod n, \quad a^{2r} \bmod n, \quad \ldots, \quad a^{2^s r} \bmod n = 1\,. \tag{2}$$

Possibly already $a^r \equiv 1 \pmod{n}$, and thus the complete sequence consists of 1's. Then we reject a without deciding on n. Otherwise the first 1 occurs at a later position. Then the element before it must be a square root of 1, but $\neq 1$. If we have bad luck, it is -1. In this case again we reject a without a decision. But if we are lucky we have found a non-trivial square root of 1, and identified n as a composite number.

Now let n be an arbitrary positive integer, and assume that $n-1$ is decomposed as in Equation (1). Then (after SELFRIDGE ca 1975) we call n a **strong pseudoprime to base** a, if

$$a^r \equiv 1 \pmod{n} \quad \text{or} \quad a^{2^k r} \equiv -1 \pmod{n} \quad \text{for a } k = 0, \ldots, s-1. \tag{3}$$

Lemma 4 (i) *A prime number is a strong pseudoprime to each base that is not a multiple of this prime.*

(ii) *A pseudoprime to base a is a forteriori a pseudoprime to base a.*

Proof. (i) If n is prime and $a^r \not\equiv 1$, then in the sequence (2) we choose k maximal with $0 \leq k < s$ and $a^{2^k r} \not\equiv 1 \pmod{n}$. Since ± 1 are the only square roots of 1 mod n we conclude $a^{2^k r} \equiv -1 \pmod{n}$.

(ii) The definition (3) immediately yields $a^{n-1} \equiv 1 \pmod{n}$. ◇

Now we face an analoguous situation as in Section 2.3 with $u = n - 1$. The set

$$B_u = \bigcup_{t=0}^{s} \{w \in \mathbb{M}_n \mid w^{r \cdot 2^t} = 1,\ \ w^{r \cdot 2^{t-1}} = -1 \text{ (if } t > 0)\}$$

exactly consists of the bases to which n is a strong pseudoprime, thus has the property $(\mathrm{E}_{n,u})$. These bases are called **prime testimonials** for n.

The Carmichael number $n = 561$ fails the test even with $a = 2$: We have $n - 1 = 560 = 16 \cdot 35$,

$$\begin{aligned} 2^{35} &\equiv 263 \pmod{561}, & 2^{70} &\equiv 166 \pmod{561}, \\ 2^{140} &\equiv 67 \pmod{561}, & 2^{280} &\equiv 1 \pmod{561}. \end{aligned}$$

Hence 561 is unmasked as a composite number since $67 \not\equiv \pm 1$. The smallest composite integer that is a strong pseudoprime to 2, 3, and 5, is $25326001 = 2251 \cdot 11251$. The only composite number $< 10^{11}$ that is a strong pseudoprime to the bases 2, 3, 5, and 7, is 3 215 031 751. This observations make us hope that the strong pseudoprime test is suited for detecting primes.

Proposition 10 *Let $n \geq 3$ be odd. Then the following statements are equivalent:*

(i) *n is prime.*

(ii) *n is a strong pseudoprime to each base a that is not a multiple of n.*

Proof. "(i) $\Longrightarrow$ (ii)": See Lemma 4 (i).

"(ii) $\Longrightarrow$ (i)": By Lemma 4 (ii) n is a prime or satisfies the definition of a Carmichael number, in particular $\lambda(n) \mid n - 1 = u$, and n is squarefree, and a forteriori not a proper prime power. Since $B_u = \mathbb{M}_n$ by assumption, Lemma 1 says that n is a prime power. Hence n is prime. $\diamond$

Corollary 2 *If n is not prime, then the number of bases $< n$ to which n is a strong pseudoprime is at most $\frac{\varphi(n)}{2}$.*

Proof. If n is a Carmichael number, then this follows from Proposition 4. Otherwise $A_u = \{w \in \mathbb{M}_n \mid w^{n-1} = 1\} < \mathbb{M}_n$ is a proper subgroup, and $B_u \subseteq A_u$. $\diamond$

With a little more care we even get the Rabin/Monier bound $\frac{\varphi(n)}{4}$ (**Exercise**).

3.3 Miller's Primality Test

How can we exploit the criterion for strong pseudoprimes to sufficiently many bases and construct a practically usable test? First we formulate the algorithm for one base a and assess its cost.

Since we anyway compute a^{n-1} by the binary power algorithm it makes sense to compute the complete sequence of powers beginning with a^r in a passing strike. Then the effort is about the same as for the "weak" pseudoprime test alone. Thus the test for strong pseudoprimes to the base a runs as follows:

```
Procedure sPPT(a)
    [Strong pseudoprime test to base $a$ ]
    Input parameters:
        $n$ = the integer to be tested (odd $\geq 3$)
        $a$ = base (in the integer interval $[2 \ldots n-1]$)
    Output parameters:
        compo = a Boolean value with the meaning
            TRUE: $n$ is composite.
            FALSE: The test has no definite result
                [i. e. $n$ is a strong pseudoprime to base $a$].
    Instructions:
        Compute $s$ = 2-order of $n-1$.
        Compute $r$ = odd part of $n-1$.
        Compute $b = a^r \bmod n$ (using the binary power algorithm).
        Set $k = 0$.
        [Loop: entry condition $b = a^{2^k r} \bmod n$
        The Boolean variable 'done', initiated with FALSE, decides
        about repeating the loop.]
        While not done:
            If $b = 1$: set done = TRUE.
                If $k = 0$: set compo = FALSE,
                else: set compo = TRUE. [1 without preceding -1]
            If $b = n-1$ and $k < s$:
                set compo = FALSE, done = TRUE.
            If $k = s$ and $b \neq 1$:
                set compo = TRUE, done = TRUE.
            In all other cases $[k < s, b \neq 1, b \neq n-1]$
                replace $b$ by $b^2 \bmod n$,
                replace $k$ by $k+1$.
```

To assess the cost we break the procedure down into single steps that each multiply two integers $\bmod n$. Computing $a^r \bmod n$ takes at most $2 \cdot \log_2(r)$ steps. In each of the up to s loops we compute a square. Since

$\log_2(n-1) = s + \log_2(r)$ we have to compute at most $2 \cdot \log_2(n)$ products $\bmod n$. Each of these squares needs at most N^2 "primitive" integer multiplications where N is the number of places of n in the used representation of the number system. Computing r takes s divisions by 2 that can be neglected. Hence a coarse estimate of the total cost yields $\mathrm{O}(\log(n)^3)$ for a single base.

MILLER's primality test is the sequence of strong peudoprime tests to the bases $2, 3, 4, 5, \ldots$. This doesn't look efficient: In the worst case we test a true prime, then we run through all bases $< n$. However as MILLER showed, significantly less bases suffice—*presupposed that the extended* RIEMANN *hypothesis is true.* In the next section we'll see some explanation but without complete proofs.

3.4 The Extended Riemann Hypothesis (ERH)

A **(complex) character** mod n is a function

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

with the properties:

1. χ has period n.
2. $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{Z}$.
3. $\chi(x) = 0$ if and only if $\mathrm{ggT}(x, n) > 1$.

The characters mod n bijectively correspond to the group homomorphisms

$$\bar{\chi} : \mathbb{M}_n \longrightarrow \mathbb{C}^\times$$

in a canonical way.

Examples are the **trivial character** $\chi(a) = 1$ for all a that are coprime with n, and the Jacobi **character** $\chi(a) = (\frac{a}{n})$ known from the theory of quadratic reciprocity, see Appendix A.5

A character defines an **L-function** by the Dirichlet series

$$L_\chi(z) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^z}.$$

This series converges absolutely and locally uniformly in the half-plane $\{z \in \mathbb{C} \mid \mathrm{Re}(z) > 1\}$ because $a^{i\cdot\mathrm{Im}(z)} = e^{i\cdot\ln(a)\cdot\mathrm{Im}(z)}$ has absolute value 1, hence

$$\left|\frac{\chi(a)}{a^z}\right| = \left|\frac{\chi(a)}{a^{\mathrm{Re}(z)} \cdot a^{i\cdot\mathrm{Im}(z)}}\right| = \frac{1}{a^{\mathrm{Re}(z)}} \qquad \text{or} \qquad = 0.$$

It admits an analytic continuation to the right half-plane $\mathrm{Re}(z) > 0$ as a holomorphic function, except for the trivial character where 1 is a simple pole.

The function L_χ has the Riemann **property** if all its zeroes in the strip $0 < \mathrm{Re}(z) \leq 1$ are on the line $\mathrm{Re}(z) = \frac{1}{2}$. The Riemann hypothesis states just this property for the Riemann zeta function, the **extended** Riemann **hypothesis (ERH)**, for all L-functions for characters mod n.

The zeta function is defined for $\mathrm{Re}(z) > 1$ by

$$\zeta(z) := \sum_{a=1}^{\infty} \frac{1}{a^z} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^z}}$$

where the last equation is Euler's product formula. Hence for the trivial character χ_1 mod n we have:

$$L_{\chi_1}(z) = \sum_{\gcd(a,n)=1} \frac{1}{a^z} \quad = \quad \zeta(z) \cdot \prod_{p|n \text{ prime}} \left(1 - \frac{1}{p^z}\right);$$

and this L-function has the same zeroes as ζ in $\mathrm{Re}(z) > 0$.

Proposition 11 (ANKENEY/MONTGOMERY/BACH) *Let $c = 2/\ln(3)^2 = 1.65707\ldots$. Let χ be a nontrivial character* $\bmod n$ *whose L-function L_χ has the* RIEMANN *property. Then there is a prime $p < c \cdot \ln(n)^2$ with $\chi(p) \neq 1$.*

We omit the proof.

Corollary 1 *Suppose ERH is true. Let $G < \mathbb{M}_n$ be a proper subgroup. Then there is a prime p with $p < c \cdot \ln(n)^2$ whose residue class* $\bmod n$ *is in the complement $\mathbb{M}_n - G$.*

Proof. There exists a nontrivial homomorphism $\mathbb{M}_n/G \longrightarrow \mathbb{C}^\times$, thus a character $\bmod n$ with $G \subseteq \ker\chi \subseteq \mathbb{M}_n$. ◇

Proposition 12 (MILLER) *Let the integer $n \geq 3$ be odd and a strong pseudoprime to all prime bases $a < c \cdot \ln(n)^2$ with c as in Proposition 11. Assume that the L-function of each character for each divisor of n has the* RIEMANN *property. Then n is prime.*

Proof. We first show that n is squarefree.

Assume $p^2 \mid n$ for some prime p. The multiplicative group $\mathbb{M}_{p^2}$ is cyclic of order $p(p-1)$. In particular the homomorphism

$$\mathbb{M}_{p^2} \longrightarrow \mathbb{M}_{p^2}, \quad a \mapsto a^{p-1} \bmod p^2,$$

is nontrivial. Its image is a subgroup $G < \mathbb{M}_{p^2}$ of order p, and is cyclic, hence isomorphic with the group of p-th roots of unity in $\mathbb{C}$. The composition of these two homomorphisms yields a character $\bmod p^2$. Thus Proposition 11 gives a prime $a < c \cdot \ln(p^2)^2$ with $a^{p-1} \not\equiv 1 \bmod p^2$. The order of a in $\mathbb{M}_{p^2}$ divides $p(p-1)$. Suppose $a^{n-1} \equiv 1 \bmod n$. Then the order also divides $n-1$. Since p is coprime with $n-1$ the order divides $p-1$, contradicting the definition of a. Hence $a^{n-1} \not\equiv 1 \bmod n$, and this in turn contradicts the strong pseudoprimality of n. Therefore n is squarefree.

Next we show that n doesn't have two different prime factors.

Assume p and q are two different prime divisors of n. Denote the 2-order of an integer x by $\nu_2(x)$. We may assume that $\nu_2(p-1) \geq \nu_2(q-1)$. Let

$$r = \begin{cases} p, & \text{if } \nu_2(p-1) > \nu_2(q-1), \\ pq, & \text{if } \nu_2(p-1) = \nu_2(q-1). \end{cases}$$

Again by Proposition 11 there is an $a < c \cdot \ln(r)^2$ with $(\frac{a}{r}) = -1$. If u is the odd part of $n-1$, and $b = a^u$, then also $(\frac{b}{r}) = -1$, in particular $b \neq 1$. By strong pseudoprimality there is a k with $b^{2^k} \equiv -1 \bmod n$. Thus b has order 2^{k+1} in $\mathbb{M}_p$ and in $\mathbb{M}_q$. In particular $2^{k+1} \mid q-1$.

In the case $\nu_2(p-1) > \nu_2(q-1)$ even $2^{k+1} \mid \frac{p-1}{2}$. We conclude $b^{(p-1)/2} \equiv 1 \pmod{p}$, but this contradicts $(\frac{b}{p}) = (\frac{b}{r}) = -1$ by EULER's criterion for quadratic residues.

In the case $\nu_2(p-1) = \nu_2(q-1)$ we have $(\frac{b}{p})(\frac{b}{q}) = (\frac{b}{r}) = -1$. Thus (without restriction) $(\frac{b}{p}) = -1$, $(\frac{b}{q}) = 1$. By EULER's criterion $b^{(q-1)/2} \equiv 1 \pmod{q}$, hence $2^{k+1} \mid \frac{q-1}{2}$, $k+2 \leq \nu_2(q-1) = \nu_2(p-1)$, hence also $b^{(p-1)/2} \equiv 1 \pmod{p}$, contradicting $(\frac{b}{p}) = -1$. $\diamond$

Therefore for MILLER's primality test it suffices to perform the strong pseudoprime test for all prime bases $a < c \cdot \ln(n)^2$. This makes total costs of $\mathrm{O}(\log(n)^5)$.

As an example, for a 512-bit integer, that is $n < 2^{512}$, testing the 18698 primes < 208704 is sufficient. Despite its efficiency this procedure takes some time. Therefore in practice this test is modified in way that is (in a sense yet to specify) not completely exact, but much faster. This is the subject of the next section.

3.5 Rabin's Probabilistic Primality Test

Rabin transferred an idea of Solovay and Strassen to Miller's test. As it later turned out Selfridge had used the method already in 1974.

If we choose a random base a in $[2 \dots n-1]$, then n "in general" fails the strong pseudoprime test to base a except when it is prime. But what means "in general"? How large is the probability? To answer this question we look at the corollary of Proposition 10 where the tighter bound $\frac{1}{4}$ was stated without proof.

Note that the bound $\frac{1}{4}$ is sharp. To see this we consider integers of the form

$$n = (1+2t)(1+4t)$$

with odd t (and assume that $p = 1+2t$ and $q = 1+4t$ are prime—example: $t = 24969$, $p = 49939$, $q = 99877$). Then $n-1 = 2r$ with $r = 3t+4t^2$, and

$$B_u = \{a \mid a^r \equiv 1 \pmod{n}\} \cup \{a \mid a^r \equiv -1 \pmod{n}\}.$$

Since $\gcd(r, p-1) = \gcd(3t+4t^2, 2t) = t = \gcd(r, q-1)$, each of these two congruences has exactly t^2 solutions. Hence $\#B_u = 2t^2$,

$$\frac{\#B_u}{n-1} = \frac{2t^2}{2\cdot(3t+4t^2)} = \frac{t}{3+4t} = \frac{1}{4+\frac{3}{t}}.$$

However most composite integers don't even come close to this bound $\frac{1}{4}$.

In general assume we are given a family $(M_{(n)})_{n\geq 1}$ of sets $M_{(n)} \subseteq [1 \dots n-1]$ and a real number $\varepsilon \in]0,1[$ with

1. $M_{(n)} = [1 \dots n-1]$ if n is prime,
2. $\#M_{(n)} \leq \varepsilon \cdot (n-1)$ for all sufficiently large odd composite integers n.

Moreover we assume that the property $a \in M_{(n)}$ is efficiently decideable for all $a \in [1 \dots n-1]$, i. e. with costs that grow at most polynomially with $\log(n)$. Then we have a corresponding (abstract) pseudoprime test:

1. Choose a random $a \in [1 \dots n-1]$.
2. Check whether $a \in M_{(n)}$.
3. Output:
   (a) If **no**: n is composite.
   (b) If **yes**: n is pseudoprime to a.

The corresponding **probabilistic primality test** consists of a series of k of these pseudoprime tests to independently chosen bases a (note that this allows for accidental repetitions). If $a \notin M_{(n)}$, we call a a witness for compositeness of n. If always $a \in M_{(n)}$ (we find no witnesses), then n is almost certainly a prime. We may assign an "error probability" δ to this event. This is computed in the following way (no it is *not* $= \varepsilon^k$):

Consider the set of odd r-bit integers, that is odd positive integers $< 2^r$. Let X be the subset of *composite* numbers, and Y_k, the subset of integers that pass the first k of a given series of independent (abstract) pseudoprime tests. The probability that a composite integer makes it into this subset is the conditional probability $P(Y_k|X) \leq \varepsilon^k$.

Nevertheless more important for the practical application is the "converse" probability $\delta = P(X|Y_k)$ that a number n that passed all the tests is still composite. This probability is assessed using BAYES' formula:

$$P(X|Y_k) = \frac{P(X) \cdot P(Y_k|X)}{P(Y_k)} \leq \frac{P(Y_k|X)}{P(Y_k)} \leq \frac{1}{q} \cdot \varepsilon^k \leq r \cdot \ln(2) \cdot \varepsilon^k,$$

where we also used the density of primes estimated by the prime number theorem:

$$P(Y_k) \geq P(\text{prime}) =: q \geq \frac{1}{r \cdot \ln(2)}$$

(the latter inequality being rather tolerant since we consider only odd numbers). Thus the "error probability" $\delta = P(X|Y_k)$ might be larger than ε^k. We can (and should) reduce it by restricting the set we search for primes, thereby enlarging $P(Y_k)$. For example before starting the series of pesudoprime tests we could try to divide by all primes say $< 100r$.

For RABIN's **primality test** we take $M_{(n)}$ as the set of bases n is a strong pseudoprime to, and $\varepsilon = \frac{1}{4}$. If n passes 25 single tests then it is prime with a quite small error probability. The probability that an exact computation produces a false result due to a hardware nor software error is larger than the error probability of RABIN's algorithm. KNUTH even doubts whether a future published proof of the extended RIEMANN hypothesis might ever be as trustworthy. Nevertheless from a mathematical viewpoint we are unsatisfied when we can't be sure that we really found a prime.

For further information on the error probability of a probabilistic primality test read

- S. H. KIM/C. POMERANCE: The probability that a random probable prime is composite. Math Comp. 53 (1989), 721–741.

- ALFRED J. MENEZES, PAUL C. VAN OORSCHOT, SCOTT A. VANSTONE: *Handbook of Applied Cryptography.* CRC Press, Boca Raton 1997, p. 147.

3.6 RSA and Pseudoprimes

To use RSA we need primes. The probabilistic Rabin primality test solves the problem of finding them in a highly efficient, but not perfectly satisfying way: We could catch a “wrong” prime. What could happen in this case?

For an analysis of the situation let $n = pq$ be a putative RSA module where p and q are not necessarily primes, but at least coprime. For the construction of the exponents d, e with

$$de \equiv 1 \pmod{\lambda(n)} \quad (\text{or} \pmod{\varphi(n)})$$

we use the possibly wrong values

$$\tilde{\varphi}(n) := (p-1)(q-1), \quad \tilde{\lambda}(n) := \mathrm{kgV}(p-1, q-1)$$

instead of the true values $\varphi(n)$ and $\lambda(n)$ of the Euler and Carmichael functions.

How do the RSA algorithms work with the “false” values? Let $a \in \mathbb{Z}/n\mathbb{Z}$ be a plaintext. As usual the case $\gcd(a, n) > 1$ leads to a decomposition of the module, we ignore it because of its extremely low probability. So we assume $\gcd(a, n) = 1$, and ask whether

$$a^{de-1} \overset{?}{\equiv} 1 \pmod{n}$$

holds. By the chinese remainder theorem this holds if and only if

$$a^{de-1} \equiv 1 \pmod{p} \quad \text{and} \quad \pmod{q}.$$

A sufficient condition is

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{and} \quad a^{q-1} \equiv 1 \pmod{q}.$$

Thus a message a might be incorrectly decrypted only if p or q is not a pseudoprime to base a. Hence:

- If instead of a prime factor p we use a Carmichael number, then RSA works correctly despite the “false” parameters, at least if a is coprime with n, though the (extremely low) probability of accidentally factorizing the module n by catching an inept plaintext a is slightly enlarged.

- Otherwise p is not a prime nor a Carmichael number. Then there is a small chance that a message cannot be correctly decrypted.

For this reason many implementations of RSA execute a few trial encryptions and decryptions after generating a key pair relying on the probabilistic Rabin test. But the effect of this additional step simply boils down to a few additional pseudoprime tests. If something goes wrong, the module is rejected.

It is unknown whether this case yet occured in this universe.

3.7 The AKS Primality Test

MILLER reduced the quest for an **efficient deterministic** primality test to the extended RIEMANN hypothesis. In August 2002 the three Indian mathematicians Manindra AGRAWAL, Neeraj KAYAL und Nitin SAXENA surprised the scientific community with a complete proof that relied on an astonishingly simple deterministic algorithm. It immediately was baptized "AKS primality test". The fastest known version costs $\mathrm{O}(\log(n)^6)$.

Proposition 13 (Basic criterion) *Let $a, n \in \mathbb{Z}$ be coprime, $n \geq 2$. Then the following statements are equivalent:*

(i) *n is prime.*

(ii) *$(X+a)^n \equiv X^n + a \pmod{n}$ in the polynomial ring $\mathbb{Z}[X]$.*

Proof. From the binomial theorem we have

$$(X+a)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} X^i$$

in $\mathbb{Z}[X]$.

"(i) $\Longrightarrow$ (ii)": If n is prime, then $n | \binom{n}{i}$ for $i = 1, \ldots, n-1$, hence $(X+a)^n \equiv X^n + a^n \pmod{n}$. By FERMAT's theorem $a^n \equiv a \pmod{n}$.

"(ii) $\Longrightarrow$ (i)": If n is composite, then we choose a prime $q|n$, and k with $q^k|n$ and $q^{k+1} \not| n$. Then $q \neq n$ and

$$q^k \not| \binom{n}{q} = \frac{n \cdots (n-q+1)}{1 \cdots q}.$$

Hence the coefficient of X^q in $(X+a)^n$ is $\neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. $\diamond$

Remarks

1. Looking at the absolute term in (ii) we see that the basic criterion generalizes FERMAT's theorem.

2. Consider the ideal $\mathfrak{q}_r := (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$ for $r \in \mathbb{N}$. If n is prime, then $(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}_r}$. This shows:

Corollary 1 *If n is prime, then in the polynomial ring $\mathbb{Z}[X]$*

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}_r}$$

for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ and all $r \in \mathbb{N}$.

Applying the basic criterion as a primality test in a naive way would cost about $\log_2 n$ multiplications of polynomials in $\mathbb{Z}/n\mathbb{Z}[X]$ using the binary power algorithm. But these multiplications become more and more expensive, in the last step we have to multiply two polynomials of degree about $\frac{n}{2}$ for an expense of size about n. The corollary bounds the degrees by $r-1$, but its condition is only necessary, not sufficient.

The sticking point of the AKS algorithm is a converse of the corollary that says that we need to try only "few" values of a, however sufficiently many, for a suitable fixed r:

Proposition 14 (AKS criterion, H. W. Lenstra**'s version)** *Let n be an integer ≥ 2. Let $r \in \mathbb{N}$ be coprime with n. Let $q := \operatorname{ord}_r n$ be the order of n in the multiplicative group $\mathbb{M}_r = (\mathbb{Z}/r\mathbb{Z})^\times$. Furthermore let $s \geq 1$ be an integer with* $\gcd(n,a) = 1$ *for all $a = 1, \ldots, s$ and*

$$\binom{\varphi(r)+s-1}{s} \geq n^{2d \cdot \lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor}$$

for each divisor $d | \frac{\varphi(r)}{q}$. Assume

$$(X+a)^n \equiv X^n + a \pmod{\mathfrak{q}} \quad \textit{for all } a = 1, \ldots s$$

with the ideal $\mathfrak{q} = \mathfrak{q}_r = (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$. Then n is a prime power.

We reproduce the proof by D. Bernstein, breaking it up into a series of lemmas and corollaries.

Lemma 5 *For all $a = 1, \ldots s$ and all $i \in \mathbb{N}$*

$$(X+a)^{n^i} \equiv X^{n^i} + a \pmod{\mathfrak{q}}.$$

Proof. We reason by induction over i. In

$$(X+a)^n = X^n + a + n \cdot f(X) + (X^r - 1) \cdot g(X)$$

we substitute $X \mapsto X^{n^i}$ in $\mathbb{Z}[X]$:

$$(X+a)^{n^{i+1}} \equiv (X^{n^i} + a)^n = X^{n^i \cdot n} + a + n \cdot f(X^{n^i}) + (X^{n^i \cdot r} - 1) \cdot g(X^{n^i})$$

$$\equiv X^{n^{i+1}} + a \pmod{\mathfrak{q}},$$

since $X^{n^i r} - 1 = (X^r)^{n^i} - 1 = (X^r - 1)(X^{r \cdot (n^i - 1)} + \cdots + X^r + 1)$ is a multiple of $X^r - 1$. $\diamond$

Now let $p|n$ be a prime divisor. *Claim*: n is a power of p.

We enlarge the ideal $\mathfrak{q} = (n, X^r - 1) \trianglelefteq \mathbb{Z}[X]$ to $\hat{\mathfrak{q}} := (p, X^r - 1) \trianglelefteq \mathbb{Z}[X]$. Then the identity from Lemma 5 holds also mod $\hat{\mathfrak{q}}$, and since we now calculate mod p, we even have:

Corollary 2 *For all $a = 1, \dots s$ and all $i, j \in \mathbb{N}$*

$$(X+a)^{n^i p^j} \equiv X^{n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Let $H := \langle n, p \rangle \leq \mathbb{M}_r$ be the subgroup generated by the residue classes $n \bmod r$ and $p \bmod r$. Let

$$d := \#(\mathbb{M}_r / H) = \frac{\varphi(r)}{\#H}.$$

From $q = \operatorname{ord}_r n \mid \#H$ we have $d \mid \frac{\varphi(r)}{q}$. Hence d satisfies the precondition of Proposition 14. For the remainder of the proof we fix a complete system of representants $\{m_1, \dots, m_d\} \subseteq \mathbb{M}_r$ of $\mathbb{M}_r/H$. Corollary 2 then extends to

Corollary 3 *For all $a = 1, \dots s$, all $k = 1, \dots, d$, and all $i, j \in \mathbb{N}$*

$$(X^{m_k}+a)^{n^i p^j} \equiv X^{m_k n^i p^j} + a \pmod{\hat{\mathfrak{q}}}.$$

Proof. We use the same trick as in Lemma 5 and substitute $X \mapsto X^{m_k}$ in $\mathbb{Z}[X]$:

$$(X+a)^{n^i p^j} = X^{n^i p^j} + a + p \cdot f(X) + (X^r - 1) \cdot g(X) \text{ in } \mathbb{Z}[X],$$

$$(X^{m_k}+a)^{n^i p^j} = X^{m_k n^i p^j} + a + p \cdot f(X^{m_k}) + (X^{m_k \cdot r} - 1) \cdot g(X^{m_k}),$$

and from this the proof is immediate. $\diamond$

The products $n^i p^j \in \mathbb{N}$ with $0 \leq i, j \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ are bounded by

$$1 \leq n^i p^j \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor}.$$

The number of such pairs $(i, j) \in \mathbb{N}^2$ is $(\lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor + 1)^2 > \frac{\varphi(r)}{d}$, and all $n^i p^j \bmod r$ are contained in the subgroup H with $\#H = \frac{\varphi(r)}{d}$. Hence there are different $(i, j) \neq (h, l)$ with

$$n^i p^j \equiv n^h p^l \pmod{r}.$$

We even have $i \neq h$—otherwise $p^j \equiv p^l \pmod{r}$, hence $p|r$. Thus we have shown the first part of the following lemma:

Lemma 6 *There exist i, j, h, l with $0 \leq i, j, h, l \leq \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor$ and $i \neq h$ such that for $t := n^i p^j$, $u := n^h p^l$, the congruence $t \equiv u \pmod{r}$ is satisfied, and $|t - u| \leq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} - 1$, as well as*

$$(X^{m_k}+a)^t \equiv (X^{m_k}+a)^u \pmod{\hat{\mathfrak{q}}}$$

for all $a = 1, \dots, s$ and all $k = 1, \dots d$.

Proof. The latter congruence follows from $X^t = X^{u+cr} \equiv X^u \pmod{X^r - 1}$, hence

$$(X^{m_k} + a)^t \equiv X^{m_k t} + a \equiv X^{m_k u} + a \equiv (X^{m_k} + a)^u \pmod{\hat{\mathfrak{q}}},$$

for all a and k. ◇

Now r and n are coprime, and p is a prime divisor of n, thus $X^r - 1$ has no multiple zeroes in an algebraic closure of $\mathbb{F}_p$. Hence it has r distinct zeroes, and these are the r-th roots of unity $\bmod\, p$. They form a cyclic group by Proposition 2. Let ζ be a generating element, that is a primitive r-th root of unity. For one of the irreducible divisors $h \in \mathbb{F}_p[X]$ of $X^r - 1$ we have $h(\zeta) = 0$. Let

$$K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X] \cong \mathbb{Z}[X]/\hat{\hat{\mathfrak{q}}}$$

with the ideal $\hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$. Thus we have an ascending chain of ideals

$$\mathfrak{q} = (n, X^r - 1) \hookrightarrow \hat{\mathfrak{q}} = (p, X^r - 1) \hookrightarrow \hat{\hat{\mathfrak{q}}} = (p, h) \trianglelefteq \mathbb{Z}[X]$$

and a corresponding chain of surjections

$$\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/\mathfrak{q} \longrightarrow \mathbb{F}_p[X]/(X^r - 1) \longrightarrow K = \mathbb{F}_p[\zeta] \cong \mathbb{F}_p[X]/h\mathbb{F}_p[X].$$

Lemma 7 *With the notations of Lemma 6 we have in K:*

(i) $(\zeta^{m_k} + a)^t = (\zeta^{m_k} + a)^u$ *for all* $a = 1, \ldots, s$ *and all* $k = 1, \ldots d$.

(ii) *If* $G \leq K^\times$ *is the subgroup generated by the* $\zeta^{m_k} + a \neq 0$, *then* $g^t = g^u$ *for all* $g \in \bar{G} := G \cup \{0\}$.

Proof. (i) follows from Lemma 6 using the homomorphism $\mathbb{Z}[X] \longrightarrow K$, $X \mapsto \zeta$ with kernel $\hat{\hat{\mathfrak{q}}} \supseteq \hat{\mathfrak{q}}$.

(ii) is a direct consequence from (i). ◇

The $X + a \in \mathbb{F}_p[X]$ for $a = 1, \ldots s$ are pairwise distinct irreducible polynomials since $p > s$ by the premises of Proposition 14. Thus also all products

$$f_e := \prod_{a=1}^{s} (X + a)^{e_a} \quad \text{for } e = (e_1, \ldots, e_s) \in \mathbb{N}^s$$

are distinct in $\mathbb{F}_p[X]$. We consider their images under the map

$$\begin{array}{rcl} \Phi\colon \mathbb{F}_p[X] & \longrightarrow & K^d, \\ f & \mapsto & (f(\zeta^{m_1}), \ldots, f(\zeta^{m_d}))\,. \end{array}$$

Lemma 8 *The images* $\Phi(f_e) \in K^d$ *of the* f_e *with* $\deg f_e = \sum_{a=1}^{s} e_a \leq \varphi(r) - 1$ *are pairwise distinct.*

Proof. Assume $\Phi(f_c) = \Phi(f_e)$. By Corollary 3 for $k = 1, \ldots, d$

$$f_c(X^{m_k})^{n^i p^j} = \prod_{a=1}^{s} (X^{m_k} + a)^{n^i p^j c_a} \equiv \prod_{a=1}^{s} (X^{m_k n^i p^j} + a)^{c_a}$$

$$= f_c(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}}$$

and likewise

$$f_e(X^{m_k})^{n^i p^j} \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\mathfrak{q}}}\,,$$

a forteriori mod $\hat{\hat{\mathfrak{q}}}$. Applying Φ to the left-hand sides yields

$$f_c(X^{m_k n^i p^j}) \equiv f_e(X^{m_k n^i p^j}) \pmod{\hat{\hat{\mathfrak{q}}}}\,.$$

Thus for the difference $g := f_c - f_e \in \mathbb{F}_p[X]$ we have $g(X^{m_k n^i p^j}) \in h\mathbb{F}_p[X]$ for all $k = 1, \ldots, d$. Let $b \in [1 \ldots r-1]$ be coprime with r, hence represent an element of $\mathbb{M}_r$. Then b is contained in one of the cosets $m_k H$ of $\mathbb{M}_r/H$. Thus there exist k, i, and j with $b \equiv m_k n^i p^j \pmod{r}$. Hence

$$g(X^b) - g(X^{m_k n^i p^j}) \in (X^r - 1)\mathbb{F}_p[X] \subseteq h\mathbb{F}_p[X],$$

hence $g(X^b) \in h\mathbb{F}_p[X]$, and $g(\zeta^b) = 0$. Thus g has the $\varphi(r)$ different zeroes ζ^b in K. But the degree of g is $< \varphi(r)$. Hence $g = 0$, and $f_c = f_e$. ◇

Corollary 4

$$\#\bar{G} \geq \binom{\varphi(r) + s - 1}{s}^{1/d} \geq |t - u| + 1.$$

Proof. There are $\binom{\varphi(r)+s-1}{s}$ options for choosing the exponents $(e_1, \ldots, e_s)$ as in Lemma 8. Since all $\Phi(f_e) \in \bar{G}^d$, we conclude

$$\#\bar{G}^d \geq \binom{\varphi(r) + s - 1}{s} \geq n^{2d \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor}$$

by the premises of Proposition 14, hence

$$\#\bar{G} \geq n^{2 \cdot \lfloor \sqrt{\frac{\varphi(r)}{d}} \rfloor} \geq |t - u| + 1$$

by Lemma 6. ◇

Now we can complete the proof of Proposition 14: Since $g^t = g^u$ for all $g \in \bar{G} \subseteq K$, the polynomial $X^{|t-u|}$ has more than $|t - u|$ zeroes in K. This is possible only if $t = u$. By the definition of t and u (in Lemma 6) n is a power of p.

This proves Proposition 14. ◇

3.8 The AKS Algorithm

We describe the algorithm in the version given by Lenstra/Bernstein. It is not trimmed to uttermost efficiency but aims at a transparent proof of polynomiality.

Input

An integer $n \geq 2$.

We measure the length of the input by the number ℓ of bits in the representation of n to base 2,

$$\ell = \begin{cases} \lceil \log_2 n \rceil, & \text{if } n \text{ is not a power of 2,} \\ k+1, & \text{if } n = 2^k. \end{cases}$$

Output

A Boolean value, coded as “COMPOSITE” or “PRIME”.

Step 1

Catch powers of 2:

- If $n = 2$: output “PRIME”, **end**.
- (Else) if n is a power of 2: output “COMPOSITE”, **end**.

  We recognize this case by $\log_2 n$ being an integer.

From now on we may assume that n is not a power of 2, and $\ell = \lceil \log_2 n \rceil$.

Step 2

We precompute a big number $N \in \mathbb{N}$ as

$$N = 2n \cdot (n-1)(n^2-1)(n^3-1)\cdots(n^{4\ell^2}-1) = 2n \cdot \prod_{i=1}^{4\ell^2}(n^i - 1).$$

This number is huge, but more importantly:

- The number $4\ell^2$ of multiplications is polynomial in ℓ.
- From
$$N \leq 2n \cdot n^{\sum_{i=1}^{4\ell^2} i} = 2n \cdot n^{\frac{4\ell^2(4\ell^2+1)}{2}} \leq 2n \cdot n^{16\ell^4},$$
  we conclude that
$$k := \lceil \log_2 N \rceil \leq 1 + (16\ell^4 + 1) \cdot \ell$$
  is polynomial in ℓ.

We repeatedly use this integer k in the following. We have $N < 2^k$, and k is the smallest positive integer with this property.

Requirements

We have to find positive integers r and s that satisfy the following requirements:

1. r and n are coprime.

2. The integer interval $[1, \ldots, s]$ contains no prime divisor of n.

3. For each divisor $d \mid \frac{\varphi(r)}{q}$, where $q = \operatorname{ord}_r n$,
$$\binom{\varphi(r)+s-1}{s} \geq n^{2d \cdot \lfloor \frac{\varphi(r)}{d} \rfloor}.$$

4. The primality criterion: For all $a = 1, \ldots, s$
$$(X+a)^n \equiv X^n + a \pmod{(n, X^r - 1)}.$$

Step 3

We choose r as the smallest prime that doesn't divide N. Then r also doesn't divide n. In particular requirement 1 is satisfied.

Why can we find r with polynomial cost?

By one of the extensions of the prime number theorem, equation (2), we have
$$\prod_{p \leq 2k,\, p \text{ prime}} p = e^{\vartheta(2k)} > 2^k > N.$$
Thus not all primes $< 2k$ divide N.

With costs that are at most quadratic in $2k$, and thus polynomial in ℓ, we get the list of all primes $\leq 2k$ (using Eratosthenes' sieve).

Step 4

Set $s := r$. Then requirement 2 is not necessarily satisfied. Hence we run through the list of primes $p < r$ that is known from step 3:

- If $p = n$: Output “PRIME”, **end**.

  [This can happen only for “small” n since n grows exponentially with ℓ but r only polynomially.]

- (Else) If $p|n$: Output “COMPOSITE”, **end**.

If we reach this point in the algorithm, then s satisfies requirement 2.

Requirement 3

To prove requirement 3 we start with the observation that $q := \operatorname{ord}_r n > 4\ell^2$.

> Otherwise $n^i \equiv 1 \pmod r$ for some i with $1 \le i \le 4\ell^2$, hence $r \mid n^i - 1 \mid N$, contradiction.

Now assume d divides $\frac{\varphi(r)}{q}$. Then

$$\begin{aligned} d &\le \frac{\varphi(r)}{q} < \frac{\varphi(r)}{4\ell^2}\,, \\ 2d \cdot \lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor &\le 2d \cdot \sqrt{\frac{\varphi(r)}{d}} = \sqrt{4d\varphi(r)} < \frac{\varphi(r)}{\ell} < \frac{\varphi(r)}{{}^2\log n}\,, \\ n^{2d\cdot\lfloor\sqrt{\frac{\varphi(r)}{d}}\rfloor} &< n^{\frac{\varphi(r)}{{}^2\log n}} = 2^{\varphi(r)}. \end{aligned}$$

On the other hand $\varphi(r) \ge 2$, so

$$\binom{\varphi(r)+s-1}{s} = \binom{\varphi(r)+r-1}{r} = \binom{2\varphi(r)}{\varphi(r)+1} \ge 2^{\varphi(r)}.$$

Hence requirement 3 is satisfied.

Step 5

Next we check requirement 4,

$$(X+a)^n \equiv X^n + a \pmod{(n, X^r - 1)}$$

in a loop for $a = 1, \ldots, r$. The number of iterations is at most r, thus $\le 2k$, hence polynomial in ℓ. During each iteration we have two binary power computations, hence a total of at most 4ℓ multiplications, the factors being polynomials of degree $< r$—polynomial in ℓ—with coefficients of size $< n$, hence of bitlength polynomial in ℓ.

- If an a violates requirement 4, then output "COMPOSITE", **end**.

Otherwise all a satisfy requirement 4, therefore n is a prime power by the AKS criterion.

Step 6

Finally we must decide whether n is a proper prime power. Since the primes $\le r$ don't divide n, we only have to check in a loop for t with $1 < t < \log_r n$:

- If $\sqrt[t]{n}$ is integer: Output "COMPOSITE", **end**.

The number of iterations is $\le \ell$, and the test in each single iteration also takes polynomial cost, if we compute $\lfloor\sqrt[t]{n}\rfloor$ by a binary search in the interval $[1 \ldots n-1]$.

- If the algorithm reaches this point, output "PRIME", **end**.

This completes the proof of:

Theorem 1 *The AKS algorithm decides the primality of n with costs that depend polynomially on* $\log n$.