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

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

(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

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

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

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

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

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**).