Towards a deterministic polynomial-time Primality Test

Neeraj Kayal 98226, Nitin Saxena 98247
Supervisor: Dr. Manindra Agarwal *

Department of Computer Science & Engineering,
Indian Institute of Technology Kanpur,
Kanpur-208016, INDIA

Abstract

We examine a primality testing algorithm presented in [Man99] and the related conjecture in [Bha01]. We show that this test is stronger than most of the popular tests today: the Fermat test, the Solovay Strassen test and a strong form of the Fibonacci test. From this, we show the correctness of the algorithm based on a widely believed conjecture, the Extended Riemann Hypothesis. We also show that any n which is accepted by the algorithm must be an odd square-free number. Thus, it is arguably the simplest and yet the strongest test for primality.

Based on our computations and results proved in this paper we feel that unlike other tests, this test is very promising as the related conjecture seems provable.

1 Introduction

The basic aim of our project was to come up with an algorithm for determining whether an inputted number n is prime or not in time polynomial in the size of the input. This is one of the fundamental problems in algorithmic number theory with important applications in cryptography and elsewhere. A number of "efficient" algorithms for the problem are known [Mil76, Rab80, SS77, APR83]. However, the problem is not yet known to be in P: while the algorithms of [Rab80, SS77] are randomized, the algorithm of [Mil76] is in P only under an unproved number-theoretic hypothesis (there exists a "small" quadratic non-residue). All these algorithms are based on various properties of prime numbers, e.g. Fermat's Little Theorem (in [Rab80, Mil76]), number of quadratic residues in prime fields (in [SS77]) etc.

* *Email addresses:* manindra@cse.iitk.ac.in (M. Agarwal), kayaln@cse.iitk.ac.in (N. Kayal), nitins@cse.iitk.ac.in (N. Saxena).

A conjecture is presented in [Bha01] which, if true, will lead to a very simple and efficient algorithm for primality. During the analysis of the above conjecture, and the corresponding algorithm we found many interesting relations with the existing number-theoretic conjectures. We found that the conjecture in [Bha01] implies a long-standing conjecture of Pomerance. We also show that the existence of a "small" quadratic non-residue would imply the correctness of the conjecture in [Man99]. Ankeny has shown in [Ank52] that the famous analytic hypothesis, the extended Riemann Hypothesis would imply the existence of the desired small quadratic non-residues in prime fields. [Bac90] generalizes this to include composite rings Z_n. Thus ERH, which is widely believed to be true by mathematicians, would imply the correctness of our algorithm. Finally, we give an apparently stronger but equivalent form of the conjecture in [Bha01].

For simplicity we will use the phrase "n, r passes our test" for:

$$(x-1)^n \equiv x^n - 1 \pmod{n, x^r - 1}$$

In section 3 we show that if n, r passes our test then n also satisfies the Fermat's test for base r. In fact we prove a much stronger assertion which is the basis of the Solovay-Strassen test:

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

where, $\left(\frac{r}{n}\right)$ refers to the Jacobi symbol. Thus, our test is strictly stronger than the Solovay-Strassen test. This allows us to prove the correctness of our algorithm on the assumption of the ERH.

In section 4 we show that if $n, 5$ passes our test then n also satifies the stronger form of the Fibonacci test:

$$\begin{aligned} F_n - \left(\frac{n}{5}\right) &\equiv 0 \pmod{n} \\ \text{and } F_{n-\left(\frac{n}{5}\right)} &\equiv 0 \pmod{n} \end{aligned}$$

Pomerance has conjectured that only composite numbers n satisfying $n^2 = 1 \pmod{5}$ can pass both the strong Fibonacci test and the Fermat test. This shows that the conjecture in [Bha01] is a generalized form of Pomerance's conjecture. We have experimentally verified the conjecture in [Bha01] for $r = 5$ for n upto 10^{11} and the conjecture has held true.

In section 5 we show that if an n passes our test for $2 \le r \le O(log^2 n)$ then n must be square-free. *To the best of our knowledge, this is the only primality testing algorithm which guarantees that any composite n which manages to pass the test is at least square-free.* In general, the problem of testing whether a number n is square free or not is believed to be as difficult as factorization itself.

In section 6 we present some approaches and insights into our conjecture and test. We explore some interesting properties of the order of $(x-1) \pmod{\frac{x^r-1}{x-1}, n}$ and using this we are able to prove our longstanding observation that only odd n's satisfy the test. We also define a set of *Introspective numbers* closely related to our test and prove that it is infact an abelian group isomorphic to a subgroup of Z_r^*. This interestingly is a cyclic group if r is prime.

Computationally we have verified the conjecture for all $n \leq 10^{11}$ and $r = 5$; and also for all $n \leq 10^{10}$ and all prime $r \leq 100$. We have also observed that for $r >= 5$, only squarefree n's satisfy our test; however we are unable to prove it as of now. We compared our test with the most popular primality test, the Miller-Rabin test and found that for any r, the pseudoprimes for our test are much larger and rarer than the Miller-Rabin pseudoprimes to base r.

2 The test

2.1 Algorithm B

Input: odd $n > 1$
Output: 1 if n is prime and 0 otherwise

if ($2^{\frac{n-1}{2}}$!= $(-1)^{\frac{n^2-1}{8}}$ (mod n)) output 0;
for r = 2 to $4(log^2\ n)$ {

    if ($r|n$) output 0;
    if ($(x-1)^n$!= x^n - 1 (mod x^r -1, n)) output 0;
}
output 1;

---

3 Relation with Strassen-Solovay's test

Definition 3.1. Henceforth, we will say that $T(n,r)$ *holds* if $(x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}$.

In this section we show that if an n passes an iteration r of B then $r^{\frac{n-1}{2}} \equiv \left(\frac{r}{n}\right) \pmod{n}$, where $\left(\frac{r}{n}\right)$ is the Jacobi symbol.

Lemma 3.1. *[Gauss' Lemma] Let a be coprime to a prime r, and let v be the number of integers greater than $\frac{r}{2}$ in the sequence: $a, 2a, \ldots.., (\frac{r-1}{2})a \pmod{r}$ then*

$$\left(\frac{a}{r}\right) = (-1)^v$$

Proof: Consider the sequence: $a, 2a, \ldots.., (\frac{r-1}{2})a$ (modulo r). Let $s_1, s_2 \ldots. s_u$ be the numbers which are $< \frac{r}{2}$ and let $l_1, l_2 \ldots. l_v$ be the numbers which are $> \frac{r}{2}$. Note that $s_1, \ldots., s_u, r - l_1, \ldots., r - l_v$ is just a permutation of $1, 2, \ldots., \frac{r-1}{2}$.

Thus,

$$\begin{aligned}
(-1)^v.s_1....s_u.l_1....l_v &\equiv (\frac{r-1}{2})! \text{ (mod } r) \\
(-1)^v.(\frac{r-1}{2})!a^{\frac{r-1}{2}} &\equiv (\frac{r-1}{2})! \text{ (mod } r) \\
a^{\frac{r-1}{2}} &\equiv (-1)^v \text{ (mod } r)
\end{aligned}$$

But when r is prime we know that $a^{\frac{r-1}{2}} \equiv \left(\frac{a}{r}\right)$ (mod r) □

Lemma 3.2. *Let a be coprime to an odd prime r. The sum of all numbers greater than* $\frac{r}{2}$ *in the sequence:* $a, 2a, ..., (\frac{r-1}{2})a$ *(modulo r) is congruent to* $(1-a)16^{-1}$ *(mod r).*

Proof: Using the notation of Lemma 3.1, we get

$$s_1 + ... + s_u - l_1 - .... - l_v \equiv 1 + 2 + ... + \frac{r-1}{2} \equiv -8^{-1} \text{ (mod } r)$$

also,

$$s_1 + ... + s_u + l_1 + ... + l_v \equiv (1 + 2 + ... + \frac{r-1}{2})a \equiv -8^{-1}a \text{ (mod } r)$$

On taking the difference of the two congruences,

$$2(l_1 + ... + l_v) \equiv 8^{-1}(1-a) \text{ (mod } r)$$

and thus we are done. □

Definition 3.2. Denote $\frac{x^r-1}{x-1}$ by $C_r(x)$.

Lemma 3.3. *If r is prime then* $(x-1)(x^2-1)....(x^{r-1}-1) \equiv r$ *(mod* $C_r(x)$*)*

Definition 3.3. Let $b = 16^{-1}$ (mod r).
Let $P_r(x) = x^b(x-1)(x^2-1)....(x^{\frac{r-1}{2}}-1)$.
For a given odd prime r and k coprime to r, let $E_k(x) = P_r(x^k)$.

Lemma 3.4. $E_k(x) \equiv \left(\frac{k}{r}\right) E_1(x)$ *(mod* $C_r(x)$*)*

Proof: Consider the sequence: $k, 2k, ..., (\frac{r-1}{2})k$ (modulo r). Let $s_1, s_2....s_u$ be the numbers which are $< \frac{r}{2}$ and let $l_1, l_2....l_v$ be the numbers which are $> \frac{r}{2}$. Now

$$E_k(x) \equiv x^{kb}(x^{s_1}-1)....(x^{s_u}-1)(x^{l_1}-1)....(x^{l_v}-1) \text{ (mod } C_r(x))$$

$$E_k(x) \equiv x^{\{kb+l_1+...+l_v\}}(-1)^v(x^{s_1}-1)....(x^{s_u}-1)(x^{r-l_1}-1)....(x^{r-l_v}-1) \text{ (mod } C_r(x))$$

Note that $s_1, ..., s_u, r-l_1, ..., r-l_v$ is just a permutation of $1, 2, ..., \frac{r-1}{2}$.
By Lemma 3.1 and Lemma 3.2, we get

$$E_k(x) \equiv x^b \left(\frac{k}{r}\right) (x-1)(x^2-1)....(x^{\frac{r-1}{2}}-1) \text{ (mod } C_r(x))$$

$$E_k(x) \equiv \left(\frac{k}{r}\right) E_1(x) \pmod{C_r(x)}$$

□

Lemma 3.5. *If r is odd prime then $E_1(x) \equiv y$ $(mod\ C_r^+(x))$*

$$where,\ y = \begin{cases} \sqrt{r} & , \quad if\ r{=}1\ (mod\ 4) \\ -\sqrt{-r} & , \quad if\ r{=}3\ (mod\ 4) \end{cases}$$

$$and\ C_r^+(x) = \Pi\{(x-\omega^k) | \left(\frac{k}{r}\right) = 1, \omega = e^{i\frac{2\pi}{r}}\}$$

Proof: Let $\omega = e^{i\frac{2\pi}{r}}$. We have, $(\omega-1)(\omega^2-1)....(\omega^{r-1}-1) = r$
thus,

$$(\omega-1)(\omega^2-1)....(\omega^{\frac{r-1}{2}}-1)\omega^{\frac{r+1}{2}}(1-\omega^{\frac{r-1}{2}})\omega^{\frac{r+3}{2}}(1-\omega^{\frac{r-3}{2}})....\omega^{r-1}(1-x) = r$$

$$\text{or, } \omega^{\{\frac{r+1}{2}+\frac{r+3}{2}+(r-1)\}}(-1)^{\frac{r-1}{2}}\{(\omega-1)(\omega^2-1)....(\omega^{\frac{r-1}{2}}-1)\}^2 = r$$

$$\text{or, } \{\omega^b(\omega-1)(\omega^2-1)....(\omega^{\frac{r-1}{2}}-1)\}^2 = (-1)^{\frac{r-1}{2}}r$$

$$\text{whence, } E_1(\omega) = \begin{cases} \sqrt{r} & , \quad \text{if r=1(mod 4)} \\ -\sqrt{-r} & , \quad \text{if r=3(mod 4)} \end{cases}$$

Now using Lemma 3.4, we get $E_1(x) \equiv y(\bmod C_r^+(x))$

$$\text{where, } y = \begin{cases} \sqrt{r} & , \quad \text{if r=1(mod 4)} \\ -\sqrt{-r} & , \quad \text{if r=3(mod 4)} \end{cases}$$

□

Corollary 3.0.1. $E_1(x) \equiv -y($ *mod* $C_r^-(x))$

$$where,\ C_r^-(x) = \Pi\{(x-\omega^k) | \left(\frac{k}{r}\right) = -1, \omega = e^{i\frac{2\pi}{r}}\}$$

Theorem 3.1. *If r is* odd *prime and $T(n,r)$ holds then*

$$r^{\frac{n-1}{2}} \equiv (-1)^{\frac{r-1}{2}\cdot\frac{n-1}{2}} \left(\frac{n}{r}\right) \quad (mod\ n)$$

Proof: Since $T(n,r)$ holds, we have

$$(x-1)^n \equiv x^n - 1 \text{ (mod } n, C_r(x))$$

Let $b = 16^{-1}$ (mod r). On substituting $x, x^2, \ldots .x^{\frac{r-1}{2}}$ in place of x above and then multiplying all the congruences we get

$$E_1(x)^n \equiv E_n(x) \text{ (mod } n, C_r(x))$$

Invoking Lemma 3.4, we get

$$E_1(x)^n \equiv \left(\frac{n}{r}\right) E_1(x) \text{ (mod } n, C_r(x))$$

$$\text{or } E_1(x)^{n-1} \equiv \left(\frac{n}{r}\right) \text{ (mod } n, C_r(x))$$

We finally get the result by using Lemma 3.5 which states that

$$E_1(x) \equiv y \text{ (mod } C_r^+(x))$$

$$\text{where, } y = \begin{cases} \sqrt{r} & , \quad \text{if r=1 (mod 4)} \\ -\sqrt{-r} & , \quad \text{if r=3(mod 4)} \end{cases}$$

□

Remark 3.1.1. Note that this gives us an alternative proof of the famous **Quadratic Reciprocity Law** for primes, since T(n,r) trivially holds if n and r are both prime.

Also, using Quadratic Reciprocity Law for Jacobians, Theorem 3.1 can be re-written as:

Corollary 3.1.1. *If r is* odd *prime and $T(n,r)$ holds then*

$$r^{\frac{n-1}{2}} \equiv \left(\frac{r}{n}\right) \textit{ (mod n)}$$

Theorem 3.2. *If n and r are co-prime numbers such that $T(n,r)$ holds and*

$$2^{\frac{n-1}{2}} \equiv (-1)^{\frac{n^2-1}{8}} \textit{ (mod n)}$$

then

$$r^{\frac{n-1}{2}} \equiv \left(\frac{r}{n}\right) \textit{ (mod n)}$$

[*This is precisely Strassen-Solovay's test.*]

Proof: Let the canonical factorisation of r be $2^e.\Pi r_i^{\alpha_i}$, where all r_i are distinct odd primes. $T(n,r)$ holds implies that $T(n,r_i)$ holds. By the Corollary 3.1.1 we know that

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

Also, the hypothesis implies that

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

Since Jacobian is multiplicative, we easily get the result by multiplying the various congruences. □

Theorem 3.3. *Assuming the ERH, Algorithm B of section 2 is a Primality Test that runs in polynomial time.*

Proof. Clearly, if B outputs 0 then n is composite. If B outputs 1 then $T(n,r)$ holds for all r co-prime to n and $2 \leq r \leq 4(log^2 n)$. But then by Theorem 3.2, Strassen-Solovay test (assuming ERH) [SS77] ensures that n is indeed prime. Also, note that Algorithm B takes $O(log^9 n)$ time, if implemented naively. □

Theorem 3.4. *Let n, m and r be natural numbers such that $(n,r) = (m,r) = 1$. If*

$$(x-1)^n \equiv (x^n - 1) \ (mod\ m, x^r - 1) \ and$$

$$2^{\frac{n-1}{2}} \equiv (-1)^{\frac{n^2-1}{8}} \ (mod\ m)$$

then

$$r^{\frac{n-1}{2}} \equiv \left(\frac{r}{n}\right) \ (mod\ m)$$

Proof: The proof is based on a simple observation that in Theorem 3.1 the n in the "mod n" plays no significant part in the proof. □

4 Relation with Fibonacci test

The (stronger form) Fibonacci test for $n \equiv \pm 2 \pmod 5$ is: $n|(F_n + 1)$ and $n|F_{n+1}$, and for $n \equiv \pm 1 \pmod 5$ is: $n|F_{n-1}$ and $n|(F_n - 1)$. We show in this section that if $(n,5) = 1$ and $T(n,5)$ holds then n passes the Fibonacci test. Thus, Fibonacci test is a very specific case of our test.

Definition 4.1. We will denote $\frac{\sqrt{5}+1}{2}$ by α and $\frac{\sqrt{5}-1}{2}$ by β.
Also let F_n be the n-th Fibonacci number s.t $F_0 = 0$ and $F_1 = 1$; and G_n be the n-th Lucas number s.t. $G_0 = 2$ and $G_1 = 1$.

Definition 4.2. For negative i's, $F_i = (-1)^{i+1}F(-i)$ and $G_i = (-1)^i G(-i)$.

It is useful to remember the following relations:

Lemma 4.1. *for all* $n \epsilon Z$,

$$F(n) = F(n-1) + F(n-2)$$

$$G(n) = G(n-1) + G(n-2)$$

$$G(n) = F(n-1) + F(n+1)$$

Lemma 4.2. *For* $i \epsilon Z$,

$$\alpha^i = \frac{G_i + F_i\sqrt{5}}{2}$$

$$(-\beta)^i = \frac{G_i - F_i\sqrt{5}}{2}$$

Proof: By induction. □

Lemma 4.3. *If n is odd and* $l = \frac{n-3}{2}$ *then,*

$$(x-1)^n \equiv x^{l+3}A_l + x^{l+2}(-3A_l + B_l) + x^{l+1}(3A_l - B_l) + x^l(-A_l) \ (mod\ n, x^5 - 1)$$

$$A_l = (-\sqrt{5})^l[\alpha^{l+1} - \beta^{l+1}]$$

$$B_l = -(-\sqrt{5})^{l+1}[\alpha^l - \beta^l]$$

Proof: Refer Appendix. □

Lemma 4.4. *Using the notation of Lemma 4.3,*
if l is even:

$$A_l = 5^{\frac{l}{2}}G_{l+1}$$

$$B_l = 5^{1+\frac{l}{2}}F_l$$

if l is odd:

$$A_l = -5^{\frac{l+1}{2}}F_{l+1}$$

$$B_l = -5^{\frac{l+1}{2}}G_l$$

Proof: Simple to get using Lemma 4.2. $\square$

Lemma 4.5. *If* $(n, 10) = 1$ *and* $T(n, 5)$ *holds iff*

- *when* $n = 10k + 1$
$$A_l = 0$$
$$B_l = 1$$
- *when* $n = 10k + 3$
$$A_l = 1$$
$$B_l = 3$$
- *when* $n = 10k + 7$
$$A_l = -1$$
$$B_l = -3$$
- *when* $n = 10k + 9$
$$A_l = 0$$
$$B_l = -1$$

Proof: We already know $(x-1)^n \pmod{n, x^5-1}$ from Lemma 4.3, we just have to compare its coefficients with $(x^n - 1) \pmod{n, x^5-1}$. $\square$

On substituting the values (given in Lemma 4.4) of A_l, B_l in the various cases of Lemma 4.5 we get the following:

Lemma 4.6. *Suppose* $(n, 10) = 1$. $(x-1)^n \equiv x^n - 1$ $(mod\ n, x^5 - 1)$ *iff*

$$\begin{array}{lrcl}
when\ n = 20k+1, & 5^{\frac{n-1}{4}} F(\frac{n-1}{2} + i) & \equiv & F(i)\ (mod\ n) \\
when\ n = 20k+11, & 5^{\frac{n+1}{4}} F(\frac{n-1}{2} + i) & \equiv & -G(i)\ (mod\ n) \\
when\ n = 20k+9, & 5^{\frac{n-1}{4}} F(\frac{n-1}{2} + i) & \equiv & -F(i)\ (mod\ n) \\
when\ n = 20k+19, & 5^{\frac{n+1}{4}} F(\frac{n-1}{2} + i) & \equiv & G(i)\ (mod\ n) \\
when\ n = 20k+7, & 5^{\frac{n+1}{4}} F(\frac{n+1}{2} + i) & \equiv & -G(i)\ (mod\ n) \\
when\ n = 20k+17, & 5^{\frac{n-1}{4}} F(\frac{n+1}{2} + i) & \equiv & F(i)\ (mod\ n) \\
when\ n = 20k+3, & 5^{\frac{n+1}{4}} F(\frac{n+1}{2} + i) & \equiv & G(i)\ (mod\ n) \\
when\ n = 20k+13, & 5^{\frac{n-1}{4}} F(\frac{n+1}{2} + i) & \equiv & -F(i)\ (mod\ n)
\end{array}$$

where, i ranges over all integers.

Theorem 4.1. *If* $(n, 10) = 1$ *and* $T(n, 5)$ *holds then*
[*when* $n \equiv \pm 2$ $(mod\ 5)$] $n|(F_n + 1)$ *and* $n|F_{n+1}$
[*when* $n \equiv \pm 1$ $(mod\ 5)$] $n|F_{n-1}$ *and* $n|(F_n - 1)$

Proof: We show this for the first case of Lemma 4.6, i.e. when $n = 20k + 1$ and

$$5^{\frac{n-1}{4}} F\left(\frac{n-1}{2} + i\right) \equiv F(i) \pmod{n} \text{ ,for all i } \epsilon \text{ Z}$$

Substituting i=0, we get $F(\frac{n-1}{2}) \equiv 0 \pmod{n}$.
Substituting i=$\frac{n-1}{2}$, we get $F(n-1) \equiv 0 \pmod{n}$ as we needed.
Substituting i=1, we get $5^{\frac{n-1}{4}} F(\frac{n+1}{2}) \equiv 1 \pmod{n}$.
Substituting i=$\frac{n+1}{2}$, we get $5^{\frac{n-1}{4}} F(n) \equiv F(\frac{n+1}{2}) \pmod{n}$.

$$\text{or } 5^{\frac{n-1}{2}} F(n) \equiv 1 \pmod{n}$$

By Theorem 3.1 this means, $F(n) \equiv 1 \pmod{n}$ as we needed.

For the other cases of Lemma 4.6 a similar sequence of steps prove the theorem. □

Remark 4.1.1. It is worth mentioning here that we have not found a composite $n \leq 10^{11}$ which is $\pm 2 \pmod 5$ and for which $T(n, 5)$ holds.

5 Our test eliminates square-full n's

In this section we show that whenever algorithm B outputs 1, n has to be square-free.

Lemma 5.1. *For* prime p *and* $1 \leq i \leq mp^{\alpha-1}$, p^α *divides* $exp = \binom{mp^{\alpha-1}}{i} p^i$

Proof: Suppose β is the largest power of p dividing i and let $i = sp^\beta$. Then the term $\binom{mp^{\alpha-1}}{i}$ furnishes atleast $p^{\alpha-1-\beta}$ (if $\beta >= \alpha$ then we are anyway done). Hence, the total power of p in exp is $\alpha - 1 - \beta + sp^\beta >= \alpha$. □

Lemma 5.2. *If for some* prime p, $p^\alpha | n$ *and*

$$(x-1)^n \equiv x^n - 1\ (mod\ n, x^r - 1)$$

then

$$(x-1)^{p^\alpha} \equiv x^{p^\alpha} - 1\ (mod\ p^\alpha, x^r - 1)$$

Proof: Suppose $n = mp^\alpha$. We have $(x-1)^p = (x^p - 1) + p.R(x)$. Therefore, $(x-1)^{mp^\alpha} = \{(x^p - 1) + p.R(x)\}^{mp^{\alpha-1}}$. Using Lemma 5.1, we get

$$\{(x^p - 1) + p.R(x)\}^{mp^{\alpha-1}} \equiv (x^p - 1)^{mp^{\alpha-1}} (\bmod p^\alpha)$$

Therefore, $(x-1)^{mp^\alpha} \equiv (x^p-1)^{mp^{\alpha-1}} \pmod{p^\alpha}$. Thus by the hypothesis, $(x^{mp^\alpha}-1) \equiv (x^p-1)^{mp^{\alpha-1}} \pmod{p^\alpha, x^r-1}$. By substituting $x^{p^{-1} (\bmod\ r)}$ in place of x, we get:

$$(x-1)^{mp^{\alpha-1}} \equiv (x^{mp^{\alpha-1}}-1) \pmod{p^\alpha, x^r-1}$$

By a very similar technique we get the following congruences:

$$(x-1)^{mp^{\alpha-2}} \equiv (x^{mp^{\alpha-2}}-1) \pmod{p^{\alpha-1}, x^r-1}$$

$$(x-1)^{mp^{\alpha-3}} \equiv (x^{mp^{\alpha-3}}-1) \pmod{p^{\alpha-2}, x^r-1}$$

and so on till

$$(x-1)^m \equiv (x^m-1) \pmod{p, x^r-1}$$

Thus, now we have $(x-1)^m = (x^m-1) + Q(x).(x^r-1) + p.R(x)$. Whence we get

$$(x-1)^{mp^\alpha} = \{(x^m-1) + Q(x).(x^r-1) + p.R(x)\}^{p^\alpha}$$

$$(x-1)^{mp^\alpha} \equiv \{(x^m-1) + p.R(x)\}^{p^\alpha} \pmod{x^r-1}$$

Once again using Lemma 5.1 we get:

$$(x-1)^{mp^\alpha} \equiv (x^m-1)^{p^\alpha} \pmod{p^\alpha, x^r-1}$$

Thus by the hypothesis, $(x^{mp^\alpha}-1) \equiv (x^m-1)^{p^\alpha} \pmod{p^\alpha, x^r-1}$. By substituting $x^{m^{-1} (\bmod\ r)}$ in place of x, we get:

$$(x-1)^{p^\alpha} \equiv (x^{p^\alpha}-1) \pmod{p^\alpha, x^r-1}$$

$\square$

Lemma 5.3. *If* $(x-1)^{p^\alpha} \equiv (x^{p^\alpha}-1)(\ mod\ p^\alpha, x^r-1)$ *then*

$$(x-1)^p \equiv (x^p-1)(\ mod\ p^\alpha, x^r-1)$$

Proof: We have $(x-1)^p = (x^p-1) + p.R(x)$. Therefore, $(x-1)^{p^\alpha} = \{(x^p-1) + p.R(x)\}^{p^{\alpha-1}}$. Using Lemma 5.1 stated above, we get

$$\{(x^p-1) + p.R(x)\}^{p^{\alpha-1}} \equiv (x^p-1)^{p^{\alpha-1}} (\bmod\ p^\alpha)$$

Thus by the hypothesis, $(x^{p^\alpha}-1) \equiv (x^p-1)^{p^{\alpha-1}} (\bmod\ p^\alpha, x^r-1)$. By substituting $x^{p^{-1} (\bmod\ r)}$ in place of x, we get:

$$(x-1)^{p^{\alpha-1}} \equiv (x^{p^{\alpha-1}}-1) (\bmod\ p^\alpha, x^r-1)$$

Raising both sides by p and using the hypothesis, we get that

$$(x^{p^{\alpha-1}} - 1)^p \equiv (x^{p^\alpha} - 1)(\bmod p^\alpha, x^r - 1)$$

and by our old technique we thus get that

$$(x-1)^p \equiv (x^p - 1)(\bmod p^\alpha, x^r - 1)$$

□

Lemma 5.4. *Number of solutions of the congruence* $x^{p-1} \equiv 1(\ mod\ p^2)$ *is atmost* $(p-1)$.

Proof: Suppose there are p solutions to this congruence. Then clearly two solutions a and b exist such that $b = a + kp$ where k is a natural number. Now, $b \equiv b^p \equiv (a+kp)^p \equiv a^p \equiv a(\bmod p^2)$, which is a contradiction. □

Theorem 5.1. *If algorithm B outputs 1 then n is* square-free.

Proof: Suppose that for some prime p, p^2 divides n. By invoking Lemma 5.2 and Lemma 5.3 we can say that $(x-1)^p \equiv (x^p - 1)(\bmod p^2, x^r - 1)$ for all prime r's, $2 \leq r \leq 4log^2p$. By Theorem 3.4 we can say that $r^{p-1} \equiv 1(\bmod p^2)$ for all prime r's, $2 \leq r \leq 4log^2p$. Notice that all such r's and the product of the powers of these r's also satisfy $x^{p-1} \equiv 1(\bmod p^2)$. By [Bru66] the number of all such solutions of $x^{p-1} \equiv 1(\bmod p^2)$ is $\psi(p^2, log^2p^2) \approx (p^2)^{1-\frac{1}{2}+o(1)}$ [where $\psi(x,y)$ denotes the number of numbers smaller than x and whose prime factors are all smaller than y].[1] Thus, the number of solutions of $x^{p-1} \equiv 1(\bmod p^2)$ exceeds p which contradicts Lemma 5.4. □

6 Conjecture and some approaches

6.1 The conjecture

We have observed empirically for a large number of pairs (n,r) [2] that whenever r is prime, n is composite and T(n,r) holds then

$$n^2 \equiv 1 \pmod r$$

Clearly, the conjecture if true would make Algorithm B a polynomial-time Primality Test.

[1] The more general result is $\psi(x, log^c x) \approx x^{1-\frac{1}{c}+o(1)}$.

[2] we have checked for all $n \leq 10^{10}$ and primes $r \leq 100$

6.2 Exploring the order of $(x-1)$

Denote $\frac{x^r-1}{x-1}$ by $C_r(x)$. Also, let the order of $(x-1) \pmod{n, C_r(x)}$ be denoted by $c_{n,r}$. Thus,

$$(x-1)^{c_{n,r}} \equiv 1 \pmod{n, C_r(x)}$$

It is simple to see that

Lemma 6.1. *$c_{n,r}$ exists for all co-prime n and r.*

Proof: Since, there are a finite number of polynomials in the ring $\pmod{n, C_r(x)}$ and inverse of $(x-1)$ exists in the ring. □

We also get the following simple result by the definition of $c_{n,r}$.

Lemma 6.2. *If n is square-free, then*

$$c_{n,r} = lcm_{p_i|n} c_{p_i,r}$$

Theorem 6.1. *$c_{n,r}$ is even and $r|c_{n,r}$.*

Proof: We have,

$$(x-1)^{c_{n,r}+1} \equiv x-1 \pmod{n, x^r-1}.$$

Assume $c_{n,r}+1 \equiv n_0 \pmod{r}$. Now let us consider the coefficients of x^i, for $0 \le i \le r-1$, in

$$(x-1)^{c_{n,r}+1} \pmod{n, x^r-1}.$$

For simplicity let us use c instead of $c_{n,r}$.

$$\text{coeff}(x^0) = [(-1)^{n_0}\binom{c+1}{n_0} + ... + (-1)^{c+1}\binom{c+1}{c+1}] \pmod{n}$$

$$\text{coeff}(x^{n_0}) = [(-1)^{c+1-n_0}\binom{c+1}{c+1-n_0} + ... + (-1)^0\binom{c+1}{0}] \pmod{n}$$

Now there are two cases:
Case 1: $c+1$ is odd.
We have coeff(x^{n_0}) = - coeff(x^0) = 1. Thus, $n_0 = 1$ or $r|c_{n,r}$ and we are done.
Case 2: $c+1$ is even.
We have coeff(x^{n_0}) = coeff(x^0) = -1. Thus, $n_0 = 0$ or $r|(c_{n,r}+1)$.

$$\text{coeff}(x^1) = [(-1)^c\binom{c+1}{c} + ... + (-1)^{r-1}\binom{c+1}{r-1}] \pmod{n}$$

$$\text{coeff}(x^{r-1}) = [(-1)^{c+1-r+1}\binom{c+1}{c+1-r+1} + ... + (-1)^1\binom{c+1}{1}] \pmod{n}$$

Therefore, coeff(x^{r-1}) = coeff(x^1) = -1 which is absurd (as coeff(x^{r-1})=0). Hence, *case 2* is **not** possible and we are done. □

A very similar proof gives the following result

Corollary 6.1.1. *Given any* m, k, r *and* n, *if* $(x-1)^m \equiv x^k - 1 (mod\ n, x^r - 1)$ *then*

$$m \equiv k (mod\ r)$$

and m *is* odd.

Remark 6.1.1. This also proves that if $T(n, r)$ holds then n *cannot* be even.

6.3 Introspective numbers

Definition 6.1. k is an *introspective number* wrt (n, r) iff

$$(x-1)^k \equiv x^k - 1 \ (\text{mod}\ n, x^r - 1)$$

Also, let us denote the set of all introspective numbers modulo $c_{n,r}$ by $I_{n,r}$.

These numbers give a really different line of approach to attack the conjecture. Let us discuss some of the properties of these numbers.

Lemma 6.3. *Let* r *be a prime number and* n *is not a power of* r. *If*

$$(x-1)^k \equiv x^k - 1 \ (mod\ n, x^r - 1)$$

then r *cannot divide* k.

Proof: Suppose that the converse holds. Let $n = r^\alpha n_0$, where $\alpha >= 1$ and n_0 are numbers and $gcd(r, n_0) = 1$. Therefore,

$$(x-1)^k \equiv x^k - 1 \equiv 1 - 1 \equiv 0 \ (\text{mod}\ r^\alpha n_0, x^r - 1)$$

We will show that this is not possible. Suppose l is the least number such that

$$(x-1)^l \equiv 0 \ (\text{mod}\ n_0, x^r - 1)$$

It is easy to see that $l > r$. Let $p(x) = (x-1)^{(l-1)} \ (\text{mod}\ n_0, x^r - 1)$. Let $p(x) = a_0 + a_1 x + ... + a_{r-1} x^{r-1}$.

$$(x-1)p(x) \equiv (a_{r-1} - a_0) + (a_0 - a_1)x + (a_1 - a_2)x^2 + ... + (a_{r-2} - a_{r-1})x^{r-1} \ (\text{mod}\ n_0, x^r - 1)$$

We have from our assumption that $(x-1)p(x) \equiv (x-1)^l \equiv 0 \ (\text{mod}\ n_0, x^r - 1)$.
Therefore, $a_0 \equiv a_1 \equiv .... \equiv a_{r-1} \equiv a \ (\text{mod}\ n_0)$, where a is a number.
Since, $(x-1)^{l-1} \equiv a_0 + a_1 x + ... + a_{r-1} x^{r-1} \ (\text{mod}\ n_0, x^r - 1)$.
We deduce (by substituting $x = 1$) that $a_0 + a_1 + ... + a_{r-1} \equiv 0 \ (\text{mod}\ n_0)$ which reduces to $ar \equiv 0 \ (\text{mod}\ n_0)$. Thus, $n_0 | a$.
Therefore, $(x-1)^{l-1} \equiv a_0 + a_1 x + ... + a_{r-1} x^{r-1} \equiv 0 (\text{mod}\ n_0, x^r - 1)$. But this contradicts the minimality of l.
Thus, r (a prime) cannot divide k. □

Lemma 6.4. *Let r be* any *number and n is a not a power of r. If*

$$(x-1)^k \equiv x^k - 1 \ (mod\ n, x^r - 1)$$

then r and k are co-prime.

Proof: Suppose the converse holds i.e.

$(x-1)^k \equiv x^k - 1 \pmod{n, x^r - 1}$ such that, there is a prime p dividing gcd(r,k).

Therefore, $(x-1)^k \equiv x^k - 1 \pmod{n, x^p - 1}$. But then by Lemma 6.3, p cannot divide k. This contradicts the definition of p. □

Lemma 6.5. *Suppose n, r are co-prime. If $k \in I_{n,r}$ then $k^i (mod\ c_{n,r}) \in I_{n,r}$.*

Proof: If $(x-1)^k \equiv x^k - 1 \pmod{n, x^r - 1}$ then raise both sides by k to get

$$(x-1)^{k^2} \equiv (x^k - 1)^k \pmod{n, x^r - 1}$$

Also, by putting x^k instead of x in the first congruence gives us

$$(x^k - 1)^k \equiv x^{k^2} - 1 \pmod{n, x^r - 1}$$

Thus, k^2 is an *introspective number*. Proceeding by induction we get the desired result. □

Lemma 6.6. *Suppose n, r are co-prime. If $k \in I_{n,r}$ then $k \in Z^*_{c_{n,r}}$.*

Proof: If k is an *introspective number* wrt (n, r), by Lemma 6.4 k is co-prime to r. Thus, there exists an i such that $k^i \equiv 1 \pmod{r}$. Now by Lemma 6.5 we know that k^i is an *introspective number* which means

$$(x-1)^{k^i} \equiv x^{k^i} - 1 \pmod{n, x^r - 1}$$

$$(x-1)^{k^i} \equiv x - 1 \pmod{n, x^r - 1}$$

$$k^i \equiv 1 \pmod{c_{n,r}}$$

Thus, k is co-prime to $c_{n,r}$. □

Lemma 6.7. *Suppose n, r are co-prime. If $k \in I_{n,r}$ then k has an inverse in $I_{n,r}$.*

Proof: As in Lemma 6.5, there exists an i such that $k^i \equiv 1 \pmod{c_{n,r}}$. Thus, k^{i-1} is the inverse of k in $I_{n,r}$. □

Lemma 6.8. *Suppose n, r are co-prime. If $k_1, k_2 \in I_{n,r}$ then*

$$k_1 * k_2 (mod\ c_{n,r}) \in I_{n,r}$$

Proof: We have,

$$\begin{aligned}
(x-1)^{k_1} &\equiv x^{k_1}-1 \pmod{n, x^r-1} \text{ and} && (1)\\
(x-1)^{k_2} &\equiv x^{k_2}-1 \pmod{n, x^r-1} && (2)\\
\text{By (1), } (x-1)^{k_1*k_2} &\equiv (x^{k_1}-1)^{k_2} \pmod{n, x^r-1} && (3)\\
\text{By (2), } (x^{k_1}-1)^{k_2} &\equiv x^{k_1*k_2}-1 \pmod{n, x^r-1} && (4)\\
\text{Thus, by (3), } (x-1)^{k_1*k_2} &\equiv x^{k_1*k_2}-1 \pmod{n, x^r-1} && (5)
\end{aligned}$$

Hence, the result is proved. □

Theorem 6.2. *Suppose n, r are co-prime. $I_{n,r}$ is a subgroup of $Z^*_{c_{n,r}}$.*

Proof: Follows directly from Lemma 6.6, 6.7 and 6.8. □

Theorem 6.3. *Suppose n, r are co-prime. $I_{n,r}$ is isomorphic to a subgroup of Z^*_r.*

Proof: Suppose $k_1 \neq k_2 \pmod{c_{n,r}}$, $k_1, k_2 \in I_{n,r}$ and

$$k_1 \equiv k_2 \equiv k \pmod{r}$$

Thus, we can say that

$$(x-1)^{k_1} \equiv x^{k_1} - 1 \pmod{n, x^r - 1} \text{ and}$$

$$(x-1)^{k_2} \equiv x^{k_2} - 1 \pmod{n, x^r - 1}$$

$$\text{Hence, } (x-1)^{k_1} \equiv (x-1)^{k_2} \pmod{n, x^r - 1}$$

$$\text{Or, } k_1 \equiv k_2 \pmod{c_{n,r}}, \text{ which is a contradiction.}$$

This shows that all the elements of $I_{n,r}$ are **distinct modulo r**, hence the mapping $h(x) = x \pmod{r}$ will be the isomorphism. □

Corollary 6.3.1. *Suppose n, r are co-prime. $\#I_{n,r} | \phi(r)$.*

Corollary 6.3.2. *Suppose n, r are co-prime. If Z^*_r is cyclic then $I_{n,r}$ is also cyclic.*

Proof: Since, every subgroup of a finite cyclic group is also cyclic [Fra]. □

6.4 A "stronger" form of conjecture

Using the properties of $c_{n,r}$, we can show that

Theorem 6.4. *Suppose n, r are co-prime. If $T(n,r)$ holds then*

$$n^2 \equiv 1 \ (mod\ r) \ \textit{iff}\ n^2 \equiv 1 \ (mod\ c_{n,r})$$

Proof: Since $r | c_{n,r}$ by Theorem 6.1, the back implication is obvious. So let us assume that $n^2 \equiv 1 \pmod r$. Since, $T(n,r)$ holds

$$\begin{aligned} (x-1)^n &\equiv x^n - 1 \pmod{n, x^r - 1} \qquad (6)\\ \text{or } (x-1)^{n^2} &\equiv (x^n - 1)^n \pmod{n, x^r - 1} \qquad (7) \end{aligned}$$

If we substitute x^n in congruence (6), we get

$$(x^n - 1)^n \equiv x^{n^2} - 1 \pmod{n, x^r - 1}$$

$$\text{Thus, by (7) } (x-1)^{n^2} \equiv x^{n^2} - 1 \pmod{n, x^r - 1}$$

But as $n^2 \equiv 1 \pmod r$ we get

$$(x-1)^{n^2} \equiv x - 1 \pmod{n, x^r - 1}$$

Now using the definition of $c_{n,r}$ we can state that $n^2 \equiv 1 \pmod{c_{n,r}}$. □

6.5 [ERH] Our test eliminates all non-Carmichael numbers

Theorem 6.5. *Assuming the Extended Riemann Hypothesis(ERH): if Algorithm B outputs 1, then n is a Carmichael number.*

Proof: Suppose Algorithm B outputs 1 on input odd n. Let p be a prime number dividing n. By [Ank52] there exists a generator r of Z_p such that $r = O(log^2 n)$. By Theorem 3.2 $r^{n-1} \equiv 1 (\text{mod } n)$, since r is a generator of Z_p we thus have $(p-1)|(n-1)$. Also, by Theorem 5.1 n is square-free. Since, n is square-free and for all prime $p|n$, $(p-1)|(n-1)$ we conclude that n is a Carmichael number. □

Corollary 6.5.1. *[ERH] If Algorithm B outputs 1 on input n and there is a prime factor p of n such that $r|(p-1)$, then*

$$n \equiv 1 \ (mod\ r)$$

6.6 Estimating the terms of $(x+1)^n - (1+x^n)$ (mod $n, 1+x^r$)

Assume that $(x+1)^n \pmod{n, 1+x^r} = a_0 + a_1 x + ... + a_{r-1}x^{r-1}$. Here we will try to get a formula for a_i in terms of complex numbers.

Lemma 6.9. *Let $n = kr + m$. Then $x^n \equiv (-1)^k x^m$ (mod $1 + x^r$).*

Proof: The proof is simple. □

Lemma 6.10. *Let $0 \le i \le r-1$. Then*

$$a_i = \binom{n}{i} - \binom{n}{i+r} + \binom{n}{i+2r} - .... \ (mod\ n)$$

Proof: By Lemma 6.9, the coefficient of x^i in $(x+1)^n \pmod{n, 1+x^r}$ will be the sum of the coefficients of $x^i, x^{i+r}, x^{i+2r}, ...$ with proper signs. Hence the result. □

Theorem 6.6. *Let $(x+1)^n$ (mod $n, 1+x^r$) $= a_0 + a_1 x + ... + a_{r-1}x^{r-1}$, r be an odd prime, $0 \le k \le r-1$. Further let $\omega_1, \omega_2, ..., \omega_{r-1}$ be r-th roots of unity. Then*

$$a_k = (-1)^k \frac{1}{r} \sum_{i=1}^{r} \left[\omega_i^{r-k}(1-\omega_i)^n\right] \ (mod\ n)$$

Proof: Let us expand: $\sum_{i=1}^{r} \left[\omega_i^{r-k}(1-\omega_i)^n\right]$

$$= \sum_{i=1}^{r}\sum_{j=0}^{n} \left[(-1)^j \binom{n}{j} \omega_i^{j+r-k}\right]$$

$$= \sum_{j=0}^{n} \left[(-1)^j \binom{n}{j} \sum_{i=1}^{r} \omega_i^{j+r-k}\right]$$

Now $\sum_{i=1}^{r} \omega_i^{j+r-k}$ will evaluate to zero except when $j \equiv k \pmod r$ in which case the sum will be r. Thus, the double-summation evaluates to:

$$\sum_{j \equiv k \pmod{r}, j \le n} \left[(-1)^j \binom{n}{j} r\right]$$

$$= (-1)^k r \left[\binom{n}{k} - \binom{n}{k+r} + ...\right]$$

Thus, using Lemma 6.10 we get the result. □

Acknowledgements

We thank Dr. Manindra Agrawal for the constant support and guidance. His suggestions and directions were valuable at crucial stages of the project. We thank Rajat Bhattacharjee for sharing his ideas with us. We also thank Carl Pomerance, H. W. Lenstra, Richard Pinch and Erich Bach for providing us their results and very useful references.

APPENDIX

Fact 1. *If n is odd and $l = \frac{n-3}{2}$ then,*

$(x-1)^n \equiv x^{l+3}A_l + x^{l+2}(-3A_l + B_l) + x^{l+1}(3A_l - B_l) + x^l(-A_l)\ (mod\ n, x^5-1)$

$$A_l = (-\sqrt{5})^l[\alpha^{l+1} - \beta^{l+1}]$$

$$B_l = -(-\sqrt{5})^{l+1}[\alpha^l - \beta^l]$$

where, α, β are as in Definition 4.1.

Proof:

$$\begin{aligned}
(x-1)^n &= (x-1)^{n-5}(x-1)^5 \ (\mathrm{mod}\ n, x^5-1) \\
&= (x-1)^{n-5}(-5x^4 + 10x^3 - 10x^2 + 5x) \ (\mathrm{mod}\ n, x^5-1) \\
&= (x-1)^{n-5}(-5)x(x-1)[(x-1)^2 + x] \ (\mathrm{mod}\ n, x^5-1) \\
&= (-5)x(x-1)^{n-2} + (-5)x^2(x-1)^{n-4} \ (\mathrm{mod}\ n, x^5-1)
\end{aligned}$$

Thus, on solving it recursively, we get

$$(x-1)^n \equiv A_k x^k (x-1)^{n-2k} + B_k x^{k+1}(x-1)^{n-2k-2} \ (\mathrm{mod}\ n, x^5-1)$$

Thus,

$$\begin{aligned}
(x-1)^n &\equiv A_k x^k[(-5)x(x-1)^{n-2k-2} + (-5)x^2(x-1)^{n-2k-4}] + B_k x^{k+1}(x-1)^{n-2k-2} \ (\mathrm{mod}\ n, x^5-1) \\
&\equiv x^{k+1}(x-1)^{n-2k-2}[-5A_k + B_k] + x^{k+2}(x-1)^{n-2k-4}[-5A_k] \ (\mathrm{mod}\ n, x^5-1)
\end{aligned}$$

A_{k+1}, B_{k+1} can be expressed in terms of A_k, B_k as

$$A_{k+1} = -5A_k + B_k$$

$$B_{k+1} = -5A_k$$

Also, we have $A_1 = -5$ and $B_1 = -5$.

The solution to this recurrence is

$$A_k = (-\sqrt{5})^k[\alpha^{k+1} - \beta^{k+1}]$$

$$B_k = -(-\sqrt{5})^{k+1}[\alpha^k - \beta^k]$$

Now

$$(x-1)^n \equiv A_l x^l (x-1)^{n-2l} + B_l x^{l+1}(x-1)^{n-2l-2} \pmod{n, x^5-1}$$

$$(x-1)^n \equiv A_l x^l (x-1)^3 + B_l x^{l+1}(x-1) \pmod{n, x^5-1}$$

$$(x-1)^n \equiv x^{l+3}A_l + x^{l+2}(-3A_l + B_l) + x^{l+1}(3A_l - B_l) + x^l(-A_l) \pmod{n, x^5-1}$$

□

References

[Bha01] Rajat Bhattacharjee, Prashant Pandey. B.Tech Report. April 2001. *Department of Computer Science & Engineering*, IIT Kanpur, INDIA.

[Man99] Manindra Agarwal, Somenath Biswas. Primality and Identity Testing via Chinese Remaindering. *IEEE conference on Foundations of Computer Science*, 1999.

[Fra] John B. Fraleigh. A first course in abstract algebra. *Narosa*, 1990.

[Her] I.N.Herstein. Topics in Algebra. *Wiley Eastern Limited.*

[Cor] Cormen et al. Introduction to Algorithms. *Prentice Hall of India.*

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comp. System Sci.* 13 (1976), 300–317.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory* 12 (1980), 128–138.

[SS77] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6 (1977), 84–86.

[APR83] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. Math.* 117 (1983), 173–206.

[Bru66] N. G. de Bruijn. On the number of positive integers $\leq$ x and free of prime factors $>$ y. *Indag. Math.* 28 (1966), 239–247.

[Ank52] N. C. Ankeny. The least quadratic non-residue. *Annals of Mathematics* 55 (1952), 65–72.

[Bac90] E. Bach. Explicit Bounds for Primality Testing and Related Problems. *Mathematics of Computation* 55 (1990), 355–380.