During the preparation of the paper the author was supported by National Science Foundation under grant MCS-8305382.

ON THE EFFICIENCY OF PROBABILISTIC PRIMALITY TESTS

Evangelos Kranakis

Department of Computer Science, Yale University

Technical Report 314, April 1984

ON THE EFFICIENCY OF PROBABILISTIC PRIMALITY TESTS

Evangelos Kranakis[1]
Department of Computer Science
Yale University

April 1984

Abstract

Let n be composite > 9. Rabin's probabilistic primality test is based on the inequality $\Pr(R_n) \leq 1/4$, *where* R_n *is the set of all numbers* $1 \leq b < n$ *such that* $b^{n-1} = 1 \bmod n$ *and for all t, if* 2^t *divides* $n-1$ *then* $gcd(b^{d(t)}-1,n)$ *is either equal to 1 or equal to n. In the present paper new improved upper and lower bounds for the quantity* $Pr(R_n)$ *are given, which depend on the number r of prime factors of n. In particular it follows from the main theorem of the paper that* $\Pr(R_n) \leq 1/2^{r-1}$. *This also gives a simpler proof of Rabin's theorem. The performance of the Solovay-Strassen primality test can be also analyzed using similar techniques. In fact it is shown that if (n−1)/2 is odd, J(.,.) denotes the Jabobi symbol, and* $S_n = \{b < n : gcd(b,n) = 1 \text{ and } b^{(n-1)/2} = J(b,n) \bmod n\}$, *then* $\Pr(S_n) \leq 1/2^{r-1}$.

1. Introduction

In the present paper a strengthening of a theorem due to Rabin is presented (see [7]), based on which one can derive a fast probabilistic primality test. Let c(X) denote the cardinality of the set X. For each composite odd number n, let $d(t) = (n-1)/2^t$, provided that 2^t divides $n-1$. Let R_n be the set of all $1 \leq b < n$ which are relatively prime to n such that $b^{n-1} = 1 \bmod n$ and for all t, $\gcd(b^{d(t)}-1,n)$ is either equal to 1 or equal to n. Let r be the number of prime factors of n. Rabin's main theorem states that

---

[1]During the preparation of the paper the author was supported by National Science Foundation under grant MCS-8305382

Theorem: If n is composite >9, and r $\geq$ 2 then $c(R_n) \leq \phi(n)/2$

The strengthening of the above theorem which will be proved in section 4, is the following

Theorem: If n is composite >9, and r $\geq$ 2 then $c(R_n) \leq \phi(n)/2^{r-1}$

This in turn will be an immediate consequence of an even stronger theorem, which is stated as theorem 6. As an immediate corollary of the main theorem, theorem 6, one obtains not only a shorter proof of Rabin's theorem, but also that "the more composite" the number tested under Rabin's primality test is, the higher is the probability that Rabin's primality test converges to the right answer, regardless of the number of times Rabin's algorithm is applied. Hence theorem 6, and the result of section 5 will provide more evidence that Rabin's Primality Test is an efficient test for testing the compositeness of a given number. The lower bound given in theorem 6 supplies some indication on the lower bound of the speed of convergence of the test. The proof of the main theorem can be found in section 4. Section 2 includes all the prerequisites necessary to understand the main proof. In section 3 the main result is stated and is used to derive a simpler proof of Rabin's original theorem, stated as theorem 3, (notice that this part of the proof uses only the upper bound in theorem 6), as well as theorem 5. Section 5 includes Rabin's probabilistic algorithm, as well as its computational complexity. In section 6, a similar result is proved for the Solovay-Strassen primality test, under the assumption (n−1)/2 is odd. Monier has carried out similar work in [5] by determining the size of the set $M_n = \{b<n: b^{n-1} \not\equiv 1 \bmod n\} \cup \{b<n: \exists t\ (2^t \text{ divides } n-1 \text{ and } b^{d(t)} \equiv -1 \bmod n\}$. Both [3] and [6] are excellent survey articles on primality tests.

2. Notation and Prerequisites

All the number theory prerequisites neeeded in the sequel can be found in any good number theory book, e.g. [2] or [9]; for questions on complexity of number theory problems [1] is very useful. Let gcd(a,b) = the greatest common divisor of a and b, rem(a,b) = the remainder when a is divided by b, and for an r-tuple $<s_1,...,s_r>$ let $rem(b,<s_1,...,s_r>) = <rem(b,s_1),...,rem(b,s_r)>$. From now on and for the rest of this paper n will be an odd positive integer, and b will range over positive integers less than n. Let r be the number of distinct prime factors $p_1,...,p_r$ of n. For i = 1,...,r let q_i be the largest power of p_i which divides n. Let Z_n^* be the set of all integers b<n such that gcd(b,n) = 1, $\phi(n) = c(Z_n^*)$, and let $Rem_n(<q_1,...,q_r>,<s_1,...,s_r>)$ be the set of all b in Z_n^* such that $rem(b,<q_1,...,q_r>) = <s_1,...,s_r>$; for simplicity, the notation $Rem(q_1,...,q_r)$ will be used.

Let G, H be two abelian groups, and let f be an epimorphism from G onto H. The kernel K = Ker(f) of f, is the set of all elements a in G such that f(a) = the identity element of H. For a in G consider the coset K+a = {k+a: k is in K}, where + is the group operation on G. G/K is the quotient group of G modulo K. It consists of all cosets K+a, where a ranges over G. The group operation $\oplus$ on G is defined by $(K+a)\oplus(K+b) = K+(a+b)$. It is not hard to show that G/K with this operation is also an abelian group which is isomorphic to H; in fact the required isomorphism is the mapping F(K+a) = f(a). For h in H let $f^{-1}\{h\}$ be the set of all a in G such that f(a) = h. Since K is the Kernel of f, it is easy to see that $f^{-1}\{h\} = K+a$, where f(a) = h. Moreover notice that all the cosets K+a have the same cardinality, namely the cardinality of K. Hence the proof of the following homomorphism theorem has been outlined:

Lemma 1: If f is an epimorphism of the abelian group G onto the abelian group H and K is the kernel of f then the group G/K is isomorphic to the group H. Moreover c(G) = c(H)c(K), and $c(f^{-1}\{h\}) = c(K)$, for all h in H.

The above Lemma will be applied to the groups $G = Z_n^*$ and $H = Z_{q_1}^* \times ... \times Z_{q_r}^*$. Indeed by the Chinese Remainder Theorem, the mapping $f(a) = rem(a,<q_1,...,q_r>)$ is an epimorphism from G onto H. Hence the kernel K of f has size $\phi(n)/(\phi(q_1)...\phi(q_r))$. As an immediate application of lemma 1 one obtains the following:

Lemma 2: For any $<s_1,...,s_r>$ in $Z_{q_1}^* \times ... \times Z_{q_r}^*$, $c(Rem(s_1,...,s_r)) = \phi(n)/(\phi(q_1)...\phi(q_r))$.

Recall that for each q which is a power of an odd prime the multiplicative group Z_q^* is cyclic. In particular each $Z_{q_i}^*$ is cyclic. Let a_i be a generator of $Z_{q_i}^*$, for i = 1,...,r.

3. The Main Result

The purpose of the present section is to state theorem 6, and show that it easily implies Rabin's theorem (theorem 3). Based on theorem 6, one can derive a probabilistic polynomial time primality test (see section 5). This probabilistic primality test is also due to Rabin, and is inspired by Miller's test for testing primality (see [4]). As an immediate corollary of theorem 6 one also obtains not only a shorter proof of Rabin's theorem, but also that "the more composite" the number tested under Rabin's primality test is, the higher is the probability that Rabin's primality test converges to the right answer, regardless of the number of times Rabin's test is applied (see section 5).

To state the main theorem a few definitions will be needed. Let $V_n = \{b<n: b^{n-1} \not\equiv 1 \mod n\}$. Also define the set W_n, which was first considered in [4].

$W_n = \{b<n: \exists t$ (2^t divides n−1 and $1<gcd(b^{d(t)}-1,n)\} \cup V_n$.

Rabin's result is the following

Theorem 3:(Rabin) For all composite $n > 9$, $c(Z_n^* - W_n) \leq \phi(n)/4$.

Let $t_i = gcd(\phi(q_i),n-1)$, $m_i = \phi(q_i)/t_i$. For each integer m, let e(m) = the largest i such that

2^i divides m; put $e_i = e(t_i)$. Theorem 3 is derived in [7] as a consequence of the following

Theorem 4: If n is composite >9, and $r \geq 2$ then $c(Z_n^* - W_n) \leq \phi(n)/(2m_1...m_r)$

Theorem 4 will in fact follow as an easy corollary of the much stronger

Theorem 5: If n is composite >9, and $r \geq 2$ then $c(Z_n^* - W_n) \leq \phi(n)/(2^{r-1}m_1...m_r)$

This last theorem will be an immediate consequence of an even stronger theorem, which will be stated in the sequel, after some definitions.

Let $\alpha_i = \max\{e_i - e_j;\ j = 1,...,r\}$, $I = \{i \leq r : \alpha_i > 0\}$, $J = \{i \leq r : \alpha_i = 0\}$. Let $\alpha = \alpha_1 + ... + \alpha_r$, $\beta = c(J)$, and $\gamma = e_1 + ... + e_r$. Notice that the above definitions easily imply that $\gamma \geq \alpha + \beta \geq r$, and $\beta > 0$.

The main result of the paper can now be stated

Theorem 6: If n is composite >9, and $r \geq 2$ then

$$\phi(n)/(2^{\gamma}m_1...m_r) \leq c(Z_n^* - W_n) \leq \phi(n)/(2^{\alpha+\beta-1}m_1...m_r)$$

Theorem 6 implies theorem 5, because $\alpha + \beta \geq r$. It is quite obvious that theorem 5 implies theorem 4. It is an immediate consequence of the lemmas below that theorem 5 implies theorem 3 (this also gives a simpler proof of theorem 3 than the one given by Rabin). This is obvious if r is bigger than or equal to 3. Cases $r = 1$ and $r = 2$ are taken care in lemmas 7 through 9 below.

Lemma 7:(Rabin) $c(Z_n^* - V_n) \leq \phi(n)/(m_1...m_r)$

Proof: Let b be an arbitrary element of the set $Z_n^* - V_n$. It is clear that gcd(b,n) = 1, and hence gcd(b,q_i) = 1 for i = 1,...,r. SInce a_i is a generator of $Z_{q_i}^*$, there exists an $s_i < \phi(q_i)$ such that $b = a_i^{s_i} \bmod q_i$. On the other hand b is not in V_n, and hence $b^{n-1} = 1$ modn. It follows that $b^{n-1} = a_i^{s_i(n-1)} = 1$ modq_i and consequently $\phi(q_i)$ divides $s_i(n-1)$. An immediate

consequence of the definitions of t_i and m_i above is that $\gcd(m_i,n-1) = 1$. Thus m_i divides s_i, and hence $s_i = h_i m_i$, for some $h_i < \phi(q_i)/m_i$.

It has now been shown that $Z_n^* - V_n$ is a subset of the union of all sets of the form $\mathrm{Rem}(a_1^{h_1 m_1},\ldots,a_r^{h_r m_r})$, where each $h_i < \phi(q_i)/m_i$. Clearly there are $\phi(q_1)/m_1 \ldots \phi(q_r)/m_r$ such sets each of which has size exactly $\phi(n)/(\phi(q_1)\ldots\phi(q_r))$, by lemma 2. This completes the proof of the lemma

Returning to the proof of theorem 3 it can now be shown

Lemma 8: (Case $r = 1$) If $n = p^t$ is composite > 9, for some prime p, then $c(Z_n^* - V_n) \leq \phi(n)/(p^{t-1})$

proof: Notice that $\phi(n) = (p-1)p^{t-1}$, and $\gcd(\phi(n),n-1) = p-1$. Now apply the previous lemma.

Lemma 9: (Case $r = 2$) Either m_1 or $m_2 \geq 2$.

Proof: Assume on the contrary $m_1 = m_2 = 1$. It follows that $q_i = p_i$, for $i = 1,2$, and $n = p_1 p_2$. Assume without loss of generality that $p_1 < p_2$. The contradiction obtained is that $\phi(p_2) = p_2 - 1$, and hence $p_2 - 1$ divides $n-1 = p_1(p_2-1) + (p_1-1)$.

The proof of the main theorem will be exhibited in the next section.

4. Proof of the Main Result

4.1. Determining the Upper Bound

This part of the proof can be considered as a careful analysis of Rabin's original ideas (see [7]). The proof itself is an extension of the proof of Lemma 7, and the reader is advised to review the notation and proof of Lemma 7.

Let b be an element of $Z_n^*-W_n$. It follows from the definition of W_n that $b^{n-1} = 1$ modn. As in the proof of Lemma 7 one has that $b = a_i^{m_i h_i}$ modq_i. The first part of the proof is based on the following

Claim : For all i, 2^{α_i} divides h_i.

Proof of the claim: Fix an i = 1,..,r. If $\alpha_i = 0$ the claim is trivial. Thus, without loss of generality it can be assumed that $\alpha_i > 0$. Consequently, there exists an index j such that $e_i \geq e_j+1$. By assumption all the $t_1,...,t_r$ must divide n−1, and hence there exists a nonnegative integer f_i such that $e(n-1) = e_i+f_i$. Put $\gamma_i = \alpha_i+f_i = e_i-e_j + f_i$. It is an immediate consequence of the definitions that $e(d(\gamma_i)) = e_j$. Moreover one can show easily that t_j divides $d(\gamma_i)$.

As in the proof of Lemma 7 one can obtain that

$$b^{d(\gamma_i)} = 1 \text{ mod} q_i \Rightarrow$$
$$\phi(q_i) \text{ divides } h_i m_i d(\gamma_i) \Rightarrow$$
$$t_i m_i \text{ divides } h_i m_i d(\gamma_i) \Rightarrow$$
$$t_i \text{ divides } h_i d(\gamma_i) \Rightarrow$$
$$2^{e_i - e_j} \text{ divides } h_i \Rightarrow$$
$$2^{\alpha_i} \text{ divides } h_i$$

In addition one also has that

$$t_j \text{ divides } d(\gamma_i) \Rightarrow$$
$$t_j m_j \text{ divides } d(\gamma_i) m_j \Rightarrow$$
$$\phi(q_j) \text{ divides } m_j d(\gamma_i) \Rightarrow.$$

Using the fact that the order of the multiplicative group $Z_{q_j}^*$ is $\phi(q_j)$, it follows that

$$b^{d(\gamma_i)} = a_j^{h_j m_j d(\gamma_i)} = 1 \text{ mod} q_j$$

However by assumption b does not belong to the set W_n, and hence $\gcd(b^{d(\gamma_i)}-1,n)$ is either

equal to 1 or equal to n. Consequently 2^{α_i} divides h_i. This completes the proof of the claim.

The claim is now enough to show that $c(Z_n^*-W_n) \leq \phi(n)/(2^{\alpha}m_1...m_r)$, by a counting argument similar to that in the proof of Lemma 7. Hence the proof for the upper bound is complete if β is equal to 1. It can therefore be assumed without loss of generality that β is greater than 1. It is clear from the definition of J that for all i,j in J, $e_i = e_j$. Let's call e this common value of the e_j's, for j in J. Let $\gamma_j = f_j + 1$, and notice that the value of f_j does not depend on j, if j is in J. Let γ denote this common value of γ_j, for j in J. It is then clear that for all j in J, t_j does not divide $d(\gamma)$ but $t_j/2$ divides $d(\gamma)$.

As in claim 1 it can be proved that for all j in J,

$$b^{d(\gamma)} \equiv 1 \bmod q_j \Leftrightarrow$$
$$\phi(q_j) \text{ divides } h_j m_j d(\gamma) \Leftrightarrow$$
$$t_j m_j \text{ divides } h_j m_j d(\gamma) \Leftrightarrow$$
$$t_j \text{ divides } h_j d(\gamma)$$

It follows from the assumption on b that for j in J, either all the h_j are even or else all the h_j are odd.

To sum up, it has been shown that the set $Z_n^*-W_n$ is a subset of the union of all sets of the form $\text{Rem}(a_1^{h_1 m_1},...,a_r^{h_r m_r})$, where each $h_i < \phi(q_i)/m_i$, and for i in I 2^{α_i} divides h_i, while at the same time either all the $\{h_j:\ j \text{ is in } J\}$ are even or else they are all odd. As in the proof of Lemma 7 it is clear that the above union can have at most $(\phi(q_1)...\phi(q_r))/(2^{\alpha+\beta-1}m_1...m_r)$ elements. This completes the proof for the upper bound in theorem 6.

4.2. Determining the Lower Bound

Consider the multiplicative abelian groups

$H(c,q_i) = \{b \text{ in } Z^*_{q_i} : b^{d(c)} = 1 \bmod q_i\}$, and $H(c,n) = \{b \text{ in } Z^*_n : b^{d(c)} = 1 \bmod n\}$, where 2^c divides $n-1$.

It is not difficult to see that the group H(e,n) is a subset of the set $Z^*_n - W_n$, where $e = e(n-1)$. Consequently, the problem of determining a lower bound for the set $Z^*_n - W_n$ reduces to the problem of determining a lower bound on the size of the group H(e,n). This is done by determining a lower bound on the size of the groups H(c,n). It is an immediate consequence of the Chinese remainder theorem that there is an isomorphism from the group $H(c,q_1) \times \ldots \times H(c,q_r)$ onto the group H(c,n). Indeed, given $\langle x_1,\ldots,x_r \rangle$ in $H(c,q_1) \times \ldots \times H(c,q_r)$ let $f(x_1,\ldots,x_r) =$ the unique x (modn) such that $x = x_i \bmod q_i$, for all $i=1,\ldots,r$.

It follows that $c(H(c,n)) = c(H(c,q_1))\ldots c(H(c,q_r))$. Hence, the lower bound will follow from the following

Lemma 10: $c(H(c,q_i)) = \gcd(d(c),\phi(q_i))$.

Proof of Lemma 10: It is easy to see that for all a,m the congruence $ax = 0 \bmod m$ has exactly $d = \gcd(a,m)$ solutions. In fact, 0 is one of its solutions, and $x_i = i(m/d)$, where $i = 0,..,r-1$, forms a complete set of distinct modm solutions of the above congruence.

Now, to solve the congruence

$$x^{d(c)} = 1 \bmod q_i,$$

one considers the linear congruence

$$yd(c) = 0 \bmod \phi(q_i),$$

which by the previous observation must have exactly $\gcd(d(c),\phi(q_i))$ solutions. This completes

the proof of the Lemma.

It is now straightforward to see that

$$\phi(q_i)/m_i = t_i =$$
$$\gcd(n-1,\phi(q_i)) =$$
$$2^{min\{e(n-1),e(p_i-1)\}} \gcd(d(e),\phi(q_i)) =$$
$$2^{e_i} \gcd(d(e),\phi(q_i)).$$

It follows that

Corollary 11: $c(H(e,n)) = \phi(n)/(2^{\gamma}m_1...m_r)$.

This gives the desired lower bound and completes the proof of the main theorem.

5. The Rabin Primality Test

To check for membership in W_n of a given b, one argues as follows. Let $e(n-1) = e$, and write $n-1 = 2^e m$.

Compute $c_0 = b^m$ modn: by repeated squaring and multiplication in $4\log_2(n)$ steps.

For i = 1 to e repeat:

1.If $1<\gcd(c_{i-1}-1,n)<n$ then output "b is in W_n", and stop.

2.Else compute $c_i = c_{i-1}^2$ modn and goto to step 1.

Hence, testing for membership in W_n requires at most $(4+e)\log_2(n)$ steps, each of which is either a multiplication or a squaring modn.

If n is composite and $b<n$ is such that $\gcd(b,n)>1$, then $b^{n-1} \not\equiv 1$ modn. Consequently all $b<n$ which are not relatively prime to n must belong to the set V_n; hence, $Z_n^*-V_n = \{b<n: b^{n-1} = 1 \text{ modn}\}$. Based on this observation one can prove

Theorem 12: If n is composite >9, and r $\geq$ 2 then

$\phi(n)/(2^{\gamma}m_1...m_r) \leq c(\{b<n:b \text{ is not in } W_n\}) \leq \phi(n)/(2^{\alpha+\beta-1}m_1...m_r)$

Rabin's primality test, call it R, is the following

Input: an odd integer n>1.

1. Choose random b<n.
2. Check if b is in W_n.

Output:

- "composite" if b is in W_n
- "prime" if b is not in W_n

Therefore it has been proved that

Theorem 13: Let n be an odd integer, and let $n-1 = 2^e m$, where m is odd. The above algorithm requires at most $(4 + e)\log_2(n)$ steps. If n is prime then R(n) = "prime". If n is composite then **Pr**(R(n) = "prime" | n is composite) $\leq 1/4$. In addition, $\phi(n)/((n-1)2^{\gamma}m_1...m_r))$ $\leq$ **Pr**(R(n) = "prime" | n is composite) $\leq \phi(n)/((n-1)2^{\alpha+\beta-1}m_1...m_r))$

If the random choices of b are independent, then repeating the test R a sufficient number of times improves the certainty of the output on input n.

6. The Solovay-Strassen Primality Test

Just like the Rabin primality test one can analyze the performance of the Solovay-Strassen primality test. Let J(b,n) denote the Jacobi sumbol of b with respect to n (see [1], [2], [9].) The Solovay-Strassen primality test is based on the following result which determines the size of the multiplicative abelian group $S_n = \{b \text{ in } Z_n^* : b^{(n-1)/2} = J(b,n) \bmod n\}$ (see [8]).

Theorem 14: (Solovay-Strassen) $c(S_n) \leq \phi(n)/2$.

If (n−1)/2 is odd then one can improve the above theorem. For simplicity let $H_n = H(1,n)$.

Theorem 15: If $r \geq 2$, and $(n-1)/2$ is odd then either $c(S_n) = c(H_n)$ or $c(S_n) = 2c(H_n)$. In particular, $\phi(n)/(2^r m_1 \ldots m_r) \leq c(S_n) \leq \phi(n)/(2^{r-1} m_1 \ldots m_r)$.

Proof: $J(-1,n) = (-1)^{d(1)} = -1$ (see [2] or [9].) Hence, $J(-x,n) = -J(x,n)$, for all x. Let H_n^+ (resp. H_n^-) be the set of x in H_n such that $J(x,n) = 1$ (resp. $J(x,n) = -1$.) Define S_n^+, S_n^- similarly. Clearly $H_n^+ = S_n^+$, and for all x in Z_n^*, x is in S_n^- if and only if $-x$ is in S_n^+. It follows that $c(S_n) = 2c(H_n^+)$. If H_n^- is the empty set then $H_n^+ = H_n$, and the proof of the theorem is complete. Otherwise, the mapping $F(x) = J(x,n)$ is an epimorphism from the group H_n onto the multiplicative group $\{1,-1\}$, with kernel H_n^+. It follows from Lemma 1 that $c(H_n) = 2c(H_n^+) = c(S_n)$, and the proof of the theorem is complete.

Remark: The above theorem is a special case of a more general result due to Monier (see [5]): If $r \geq 2$, then $c(S_n) = \delta_n \gcd(d(1),\phi(q_1)) \ldots \gcd(d(1),\phi(q_r))$, where δ_n can take only the values 2, 1 or 1/2.

Example 1: The upper bound in theorem 17 can be attained e.g. if $n=3\cdot5=15$, then $H(1,15) = \{1\}$, and $S(1,15) = \{1,14\}$.

Example 2: There are infinitely many odd n such that $(n-1)/2$ is odd. Indeed, let n be the product of odd integers $s_1,\ldots,s_r$ such that $e(s_1-1) = 1$ but $e(s_i-1) > 1$, for all $i=2,\ldots,r$.

The Solovay-Strassen primality test, call it SS, is the following (see [1])

Input: an odd integer $n>1$.

1. Choose random $b<n$.
2. Check if b is in S_n.

Output:

- "composite" if b is not in S_n
- "prime" if b is in S_n

As before, if n is composite and b<n is such that gcd(b,n)>1, then $b^{n-1} \not\equiv 1 \bmod n$. Consequently all b<n which are not relatively prime to n must belong to the set V_n. Therefore it has been proved that

Theorem 16: Let n be an odd integer. Then in the above algorithm: if n is prime, SS(n) = "prime"; if n is composite then Pr(SS(n) = "prime" | n is composite) $\leq 1/2$. If in addition $r \geq 2$, and $(n-1)/2$ is odd then in the above algorithm: if n is composite then

$$\phi(n)/((n-1)2^{\gamma}m_1 \ldots m_r)) \leq \Pr(SS(n) = \text{"prime"} \mid n \text{ is composite}) \leq \phi(n)/((n-1)2^{\gamma-1}m_1 \ldots m_r))$$

7. Acknowledgements

Many thanks to Dan Gusfield who motivated me to prove this result, to Mike Fischer whose many valuable comments helped me improve the presentation, and to Eric Bach for making me aware of Monier's work.

8. References

[1] **D. Angluin**, Lectures Notes on the Complexity of some problems in Number Theory, Technical Report 243, Yale University, August 1982.

[2] **E. Kraetzel**, Zahlentheorie, VEB Deutscher Verlag der Wissenschaften, 1981 Berlin.

[3] **M. Mignote**, Tests de Primalite, Theoretical Computer Science 12(1980) 109-117.

[4] **G.L. Miller**, Riemann's Hypothesis and Tests for Primality, J. Comput. System Sci. 13(1976), 300-317.

[5] **L. Monier**, Evaluation and Comparison of two Efficient Probabilistic Primality Tests, Theoretical Computer Science 12(1980) 97-108.

[6] **C. Pomerance**, Recent Developments in Primality Testing, The Mathematical Intelligencer, Vol. 3. Number 3(1980), 97-105.

[7] **M.O. Rabin**, Probabilistic Algorithm for Testing Primality, J. Number Theory 12(1980), 128-138.

[8] **R. Solovay and V. Strassen**, A Fast Monte-Carlo Test for Primality, SIAM J. Comput. 6(1977), 84-85; erratum, 7(1978), 118.

[9] **I.M. Vinogradov**, Elements of Number Theory, Dover, 1954 New York.