Recognizing Primes In Random Polynomial Time

Leonard M. Adleman*

Department of Computer Science
University of Southern California

Ming-Deh A. Huang

Department of Computer Science
University of Southern California

Abstract

This paper is the first in a sequence of papers which will prove the existence of a random polynomial time algorithm for the set of primes. The techniques used are from arithemetic algebraic geometry and to a lesser extent algebraic and analytic number theory. The result complements the well known result of Strassen and Solovay that there exists a random polynomial time algoritm for the set of composites.

1 Introduction

In the words of Gauss [G]

> *The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length.*

Nonetheless, it seems appropriate to point out the impact made by the recent advent of the theory of computational complexity and with it the ability to judge clearly the effeciency of proposed methods:

1. In 1974 Pratt [P] showed that the primes were recognizable in non-deterministic polynomial time.
2. In 1974 Solovay and Strassen [SS] showed that the composites were recognizable in random polynomial time.
3. In 1974 Miller [M] showed that the Riemann hypothesis for Dirichlet L-functions implied that the primes were decidable in deterministic polynomial time.
4. In 1980 Adleman, Pomerance, and Rumely [APR] showed that there exists a $c \in \mathbf{N}$ such that the primes were decidable in deterministic time $O((\log n)^{c \log \log \log n})$.
5. In 1986 Goldwasser and Killian [GK] showed that Cramér's conjecture on gaps between primes implied that the primes were recognizable in random polynomial time.

This is the first in a sequence of papers which will prove, without hypothesis, that the primes are recognizable in random polynomial time. Our methods are primarily from arithmetic algebraic geometry. Extensive use is made of both the theory of Abelian varieteis as developed in Weil [W1] [W2], Shimura, Taniyama [ST], Honda [H], Serre, Tate [SeT], [T], Waterhouse [Wa], Mumford [Mu1], [Mu2], Faltings [F] and others; and of the algorithmic ideas of Schoof [S], Lenstra [L], Goldwasser and Killian [GK].

Formally, in this first paper we will prove the following:

Theorem 1 (Assumption 1 through 3 imply) *There exist a $c \in \mathbf{N}$ and a polynomial time computable everywhere defined function $\mathcal{F} : N^2 \rightarrow \{0,1\}$ such that both:*

1. *for all $n \in \mathbf{N}$ with n composite, for all $r \in \mathbf{N}$,*

$$\mathcal{F}(n,r) = 0$$

2. *for all $p \in \mathbf{N}$ with p prime,*

$$\frac{\#\{r : |r| \leq |p|^c \;\&\; \mathcal{F}(p,r) = 1\}}{\#\{r : |r| \leq |p|^c\}} \geq \frac{1}{2}$$

The assumptions 1 through 3 indicated above are found in section 5. The proofs of these assumptions will be the topics of the remaining papers in this sequence.

*Research supported by NSF through grant DCR 8519296

2 Algorithm

For all $r \in \mathbf{N}$ let $|r|$ denote the length of r when written in binary. It will be convienent in describing the next algorithm to have a construct for extracting an initial sequence of bits from one number to form another. Accordingly, for all $c, l, r \in \mathbf{N}$ let $c = SLICE(l, r)$ denote the sequence of instructions:

CALCULATE $a, b \in \mathbf{N}$ such that $r = a * 2^l + b$
SET $c = b$
SET $r = a$

Consider the function $\mathcal{F}$ computed by the following algorithm A, where α and $\mathcal{G}$ are as in Assumption 2 and β and $\mathcal{H}$ are as in Assumption 3:

1. *Input n,r.*

2. $r_0 = SLICE(|n|^{\alpha}, r)$
   $a_i = SLICE(|n|, r) \quad i = 0, 1, \ldots, 6$
   Calculate
   $n_1 = \mathcal{G}(< n, f_0 >, r_0)$
   where:
   $f_0 = \sum_{i=0}^{6}(a_i mod(n))x^i \in (\mathbf{Z}/n\mathbf{Z})[x]$

3. $r_1 = SLICE(|n_1|^{\alpha}, r)$
   $b_i = SLICE(|n_1|, r) \quad i = 0, 1, \ldots, 6$
   Calculate
   $n_2 = \mathcal{G}(< n_1, f_1 >, r_1)$
   where:
   $f_1 = \sum_{i=0}^{6}(b_i mod(n_1))x^i \in (\mathbf{Z}/n_1\mathbf{Z})[x]$

4. $r_2 = SLICE(|n_2|^{\alpha}, r)$
   $c_i = SLICE(|n_2|, r) \quad i = 0, 1, \ldots, 6$
   Calculate
   $n_3 = \mathcal{G}(< n_2, f_2 >, r_2)$
   where:
   $f_2 = \sum_{i=0}^{6}(c_i mod(n_2))x^i \in (\mathbf{Z}/n_2\mathbf{Z})[x]$

5. $r_3 = SLICE(|n_3|^{\beta}, r)$
   Calculate
   $d = \mathcal{H}(n_3, r_3)$

6. *Output d*

We will prove that $\mathcal{F}$ has the properties indicated in the following theorem:

Theorem 2 (Assumption 1 through 3 imply) *There exist a polynomial $g \in \mathbf{Z}[x]$, an $a \in \mathbf{N}$ and a polynomial time computable everywhere defined function $\mathcal{F} : N^2 \rightarrow \{0, 1\}$ such that both:*

1. *for all $n \in \mathbf{N}$ with n composite, for all $r \in \mathbf{N}$,*
$$\mathcal{F}(n, r) = 0$$

2. *for all sufficiently large $p \in \mathbf{N}$ with p prime,*
$$\frac{\#\{r : |r| \leq g(|p|) \ \& \ \mathcal{F}(p, r) = 1\}}{\#\{r : |r| \leq g(|p|)\}} \geq \frac{1}{\log^a(p)}$$

Theorem 1 follows easily from Theorem 2 by considering $\mathcal{F}' : N^2 \rightarrow \{0, 1\}$ defined as follows:

$$\mathcal{F}'(n, r) = 1 - \left(\prod_{i=0}^{z}(1 - \mathcal{F}(n, r_i))\right)$$

Where the r_i's are successive SLICEs of r and z is chosen appropriately.

3 Hyperelliptic Curves

By a hyperelliptic $\mathbf{F}_p$-curve C, we mean a smooth projective variety defined over $\mathbf{F}_p$ such that $\mathbf{F}_p(C)$, the field of rational functions of C defined over $\mathbf{F}_p$, is a separable quadratic extension of a purely transcendental extension of $\mathbf{F}_p$.

Two hyperelliptic $\mathbf{F}_p$-curves C_1 and C_2 are $\mathbf{F}_p$-isomorphic iff $\mathbf{F}_p(C_1) \cong \mathbf{F}_p(C_2)$. For all hyperelliptic $\mathbf{F}_p$-curves C, $[C]$ denotes the $\mathbf{F}_p$-isomorphism class of C.

For all hyperelliptic $\mathbf{F}_p$−curves C and all $f \in \mathbf{F}_p[x]$, the polynomial y^2-$f \in \mathbf{F}_p[x,y]$ is an *affine representative* for $[C]$ iff f has no multiple roots and $Q(\mathbf{F}_p[x,y]/(y^2\text{-}f))$, the field of fractions of $\mathbf{F}_p[x,y]/(y^2\text{-}f)$, is isomorphic to $\mathbf{F}_p(C)$.

In what follows we shall be considering the set of hyperelliptic $\mathbf{F}_p$−curves of genus 2. Since it is well known that this is precisely the set of $\mathbf{F}_p$−curves of genus 2 we shall drop the 'hyperelliptic' modifier.

Lemma 1 *For all $\mathbf{F}_p$−curves C of genus 2 there exists an $f \in \mathbf{F}_p[x]$ of degree 6 such that $y^2 - f$ is an affine representative for $[C]$.*

Proof It is well-known that all hyperelliptic $\mathbf{F}_p$−curves C of genus g have an affine representative $y^2 - h$ where $h \in \mathbf{F}_p[x]$ is of degree 2g+1 or 2g+2. Assume h has degree 5. By a linear change of variable if necessary, we may assume that h has no root at 0.

We have $Q\left(\mathbf{F}_p[x,y]/(y^2 - h)\right) = \mathbf{F}_p(u,v)$ where u is transcendental over $\mathbf{F}_p$ and $v^2 = h(u)$. Let $w = u^{-1}$. Then $h(u) = h(w^{-1}) = w^{-5}g(w)$ where $g \in \mathbf{F}_p[x]$ has degree 5, g has no multiple roots, and $g(0) \neq 0$. Let $z = w^3 v$ and $f = xg$. Then $z^2 = f(w)$. Further, $\mathbf{F}_p(u,v) = \mathbf{F}_p(u^{-1}, u^{-3}v) = \mathbf{F}_p(w,z)$. Since $Q\left(\mathbf{F}_p[x,y]/(y^2 - f)\right) \cong \mathbf{F}_p(w,z)$, $y^2 - f$ is the desired affine representative of $[C]$. □

It is easily shown that for all primes p and all $f \in F_p[x]$ of degree 6 without multiple roots, there exists an $\mathbf{F}_p$−curve $C = C(f)$ of genus 2 such that $y^2 - f$ is an affine representative for $[C]$. Let $\mathcal{D}(f)$ denote the number of $\mathbf{F}_p$−rational points on the Jacobian of $C(f)$.

Let $SL_2(\mathbf{F}_p)$ be the group of 2 by 2 matrices over $\mathbf{F}_p$ with determinant equal to 1.

For all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_p)$, for all fields K containing $\mathbf{F}_p$, and for all $x \in K$, define $A(x) = \frac{ax+b}{cx+d}$. Then for all $A, B \in SL_2(\mathbf{F}_p)$, $A(B(x)) = (AB)(x)$. For all $(\alpha_1, ..., \alpha_6)$ with $\alpha_i \in \overline{\mathbf{F}}_p$, define $A(\alpha_1, ..., \alpha_6) = (A(\alpha_1), ..., A(\alpha_6))$. For all $f \in \mathbf{F}_p[x]$ such that $f = a\prod_{i=1}^6 (x - \alpha_i)$, define $f^A = a\prod_{i=1}^6 (x - A(\alpha_i))$.

Lemma 2 *Let $f \in \mathbf{F}_p[x]$ be monic of degree 6 without multiple roots. Then*

1. *for all $a, b \in \mathbf{F}_p$, if there exists a $c \in \mathbf{F}_p - \{0\}$ such that $ab = c^2$ then*
$$Q(\mathbf{F}_p[x,y]/(y^2 - af)) \cong Q(\mathbf{F}_p[x,y]/(y^2 - bf))$$
2. *for all $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in SL_2(\mathbf{F}_p)$, and all $a \in \mathbf{F}_p - \{0\}$,*
$$Q(\mathbf{F}_p[x,y]/(y^2 - af)) \cong Q(\mathbf{F}_p[x,y]/(y^2 - g))$$
where $g = af(\frac{a_1}{a_3})f^{A^{-1}}$.

Proof (1) $Q\left(\mathbf{F}_p[x,y]/(y^2 - af)\right) = \mathbf{F}_p(s,t)$ with s transcendental over $\mathbf{F}_p$ and $t^2 = af(s)$. $Q\left(\mathbf{F}_p[x,y]/(y^2 - bf)\right) = \mathbf{F}_p(u,v)$ with u transcendental over $\mathbf{F}_p$ and $v^2 = bf(u)$. Since $af(u) = (b^{-1}c)^2 v^2$, there is a homomorphism from $\mathbf{F}_p(s,t)$ to $\mathbf{F}_p(u,v)$ over $\mathbf{F}_p$ sending s to u and t to $b^{-1}cv$. Since $\mathbf{F}_p(u,v) = \mathbf{F}_p(u, b^{-1}cv)$, the homomorphism is an isomorphism.
(2) $Q\left(\mathbf{F}_p[x,y]/(y^2 - af)\right) = \mathbf{F}_p(s,t)$ with s transcendental over $\mathbf{F}_p$ and $t^2 = af(s)$. $Q\left(\mathbf{F}_p[x,y]/(y^2 - g)\right) = \mathbf{F}_p(u,v)$ with u transcendental over $\mathbf{F}_p$ and $v^2 = g(u)$. It is easily verified that

$$f(A(u)) = \frac{a_3^6}{(a_3 u + a_4)^6} f(\frac{a_1}{a_3}) f^{A^{-1}}(u).$$

Hence,

$$af(A(u)) = \frac{a_3^6}{(a_3 u + a_4)^6} g(u) = \left(\left(\frac{a_3}{a_3 u + a_4}\right)^3 v\right)^2.$$

From this one sees that there is a homomorphism ϕ sending s to $A(u)$ and t to $(\frac{a_3}{a_3 u + a_4})^3 v$.

Since $A^{-1}(A(u)) = (A^{-1}A)(u) = u$, $\mathbf{F}_p(u) = \mathbf{F}_p(A(u))$. Further, $\mathbf{F}_p\left(u, (\frac{a_3}{a_3 u+a_4})^3 v\right) = \mathbf{F}_p(u,v)$. Therefore, $\mathbf{F}_p(u,v) = \mathbf{F}_p\left(u, (\frac{a_3}{a_3 u+a_4})^3 v\right)$. Hence, ϕ is an isomorphism. □

Let S_6 be the group of permutations on $\{1,2,3,4,5,6\}$. For all $(\alpha_1, ..., \alpha_6)$ with $\alpha_i \in \overline{\mathbf{F}}_p$, for all $\tau \in S_6$, let $\tau(\alpha) = (\alpha_{\tau(1)}, ..., \alpha_{\tau(6)})$, and $G_\alpha = \{A \in SL_2(\mathbf{F}_p) : A(\alpha) = \tau(\alpha)$ for some $\tau \in S_6\}$.

Lemma 3 *Let $\alpha = (\alpha_1, ..., \alpha_6)$ where α_i, $1 \le i \le 6$, are distinct elements of $\overline{\mathbf{F}}_p$. Then $[G_\alpha : 1] \le 6!2$.*

Proof For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_p)$,

$$A(\alpha) = \alpha$$

$$\Leftrightarrow$$

$$\frac{a\alpha_i + b}{c\alpha_i + d} = \alpha_i, \quad i = 1, 2, ..., 6.$$

$$\Leftrightarrow$$

$$c\alpha_i^2 + (d-a)\alpha_i - b = 0, \quad i = 1, 2, ..., 6.$$

Since the α_i's are all distinct it follows that $c = d - a = b = 0$. Consequently

$$A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

For all $\tau \in S_6$, let

$$G(\tau) = \{A \in SL_2(\mathbf{F}_p) : A(\alpha) = \tau(\alpha)\}.$$

Suppose there exists $A \in G(\tau)$, then for all $B \in SL_2(\mathbf{F}_p)$,

$$B \in G(\tau) \Leftrightarrow B(\alpha) = A(\alpha) \Leftrightarrow \alpha = (B^{-1}A)(\alpha)$$

Therefore,

$$B^{-1}A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence, $[G(\tau) : 1] \le 2$. Since

$$G_\alpha = \bigcup_{\tau \in S_6} G(\tau),$$

$$[G_\alpha : 1] \le \sum_{\tau \in S_6} [G(\tau) : 1] \le 6!2 \quad \square$$

Proposition 1 *There exists a $c \in \mathbf{R}_{>0}$ such that for all $\mathbf{F}_p$-curves C*

$$\# \left\{ f \in \mathbf{F}_p[x] : \begin{array}{l} f \text{ has degree } 6 \ \& \\ y^2 - f \text{ is an affine} \\ \text{representative for } [C] \end{array} \right\} > cp^4.$$

Proof Let

$$S = \left\{ f \in \mathbf{F}_p[x] : \begin{array}{l} \text{f has degree 6 \&} \\ y^2 - f \text{ is an affine} \\ \text{representative for } [C] \end{array} \right\}.$$

By Lemma 1, there exists a $b \in \mathbf{F}_p - \{0\}$ and a monic $f \in \mathbf{F}_p[x]$ such that $bf \in S$.

Let $\alpha = (\alpha_1, ..., \alpha_6)$, where $\alpha_1, ..., \alpha_6$ are the distinct roots of f. For all $A, B \in SL_2(\mathbf{F}_p)$, let $A \sim B$ iff $f^A = f^B$. Then $A \sim B$ iff $A(\alpha) = \tau(B(\alpha))$ for some $\tau \in S_6$ iff $B^{-1}A \in G_\alpha$. By lemma 3 and the observation that G_α is a group, there exists a $d \in \mathbf{N}$ such that there are at least p^3/d inequivalent A's.

For all $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in SL_2(\mathbf{F}_p)$, let

$$G(A) = \{a : a \in \mathbf{F}_p - \{0\} \ \& \ ba f(\frac{a_1}{a_3}) \in F_p^2\}$$

Then $\#G(A) = \frac{p-1}{2}$. By Lemma 2 and the observation that for all $A \in SL_2(\mathbf{F}_p)$, $f^{A^{-1}}$ has no multiple roots, we have that for all $A \in SL_2(\mathbf{F}_p)$, for all $a \in G(A)$,

$$af^{A^{-1}} \in S.$$

However for all $A_1, A_2 \in SL_2(\mathbf{F}_p)$, for all $a_1 \in G(A_1)$, $a_2 \in G(A_2)$

$$a_1 f^{A_1^{-1}} = a_2 f^{A_2^{-1}} \Leftrightarrow a_1 = a_2 \text{ and } A_1 \sim A_2$$

and the theorem follows. □

4 Proof of Theorem 2

For all $p \in primes$

Let

$$S(p) = \left\{ q : \begin{array}{c} q \in primes \ \& \\ p^2 - p^{1.5} \leq q \leq p^2 \ \& \\ N_C(p,q) \geq \frac{p^{1.5}}{\log^e(p)} \end{array} \right\}$$

where N_C, and e are as in Assumption 1.

Let

$$U(p) = \left\{ < p, q_1, q_2, q_3 >: \begin{array}{c} q_1 \in S(p) \ \& \\ q_2 \in S(q_1) \ \& \\ q_3 \in S(q_2) \end{array} \right\}$$

Observe that $< p, q_1, q_2, q_3 > \in U(p) \Rightarrow q_3 \leq p^8$.

Let

$$T(p) = \left\{ < p, q_1, q_2, q_3 >: \begin{array}{l} < p, q_1, q_2, q_3 > \in U(p) \\ \& \\ q_3 \notin \mathcal{E}(p^8) \end{array} \right\}$$

where $\mathcal{E}$, is as in Assumption 3.

We need a theorem concerning primes in short intervals. The following result which is a minor varient of one due to Iwaniec and Juttila [IJ] is sufficient.

Theorem 3 *There exists a $d \in \mathbf{N}$ such that for all sufficiently large $x \in \mathrm{N}$ the number of primes between x^2-$x^{1.5}$ and x^2 is greater than $x^{1.5}/log^d(x)$.*

Lemma 4 *There exists a $c \in \mathbf{N}$ such that for all sufficiently large primes p, $\#T(p) \geq p^{10.5}/log^c(p)$.*

Proof

we have

$$\#T(p) \geq \#U(p) - \sum \#V(q)$$

where:

$$V(q) = \{< p, q_1, q_2, q >: < p, q_1, q_2, q > \in U(p)\}$$

and the sum is over all $q \in \mathcal{E}(p^8)$.

By the previous theorem and Assumption 1, there exists an $a \in \mathbf{N}$ such that for all sufficiently large $p \in primes$

$$\#U(p) \geq p^{10.5}/\log^a(p).$$

By the definition of S we have that

$$< p, q_1, q_2, q > \in V(q)$$

$$\Downarrow$$

$$q^{\frac{1}{2}} \leq q_2 \leq q^{\frac{1}{2}} + q^{\frac{1}{4}} \ and \ q^{\frac{1}{4}} \leq q_1 \leq q^{\frac{1}{4}} + q^{\frac{1}{8}}.$$

It follows that for all $q \in \mathcal{E}(p^8)$, $\#V(q) \leq p^3$.

By Assumption 3 there exists a $\delta \in \mathbf{R}$ with $\delta < 7.5$ such that $\mathcal{E}(p^8) \leq p^\delta$ and the result follows.□

Proof of Theorem 2

Part 1 follows immediately from Assumptions 2 and 3.

For part 2, assume p is prime and let

$$g = (49 + 7\alpha + 8\beta)x$$

where α and β are as in Assumptions 2 and 3. We will show that g has the desired property.

First, there exists a $c_0 \in \mathbf{N}$ such that

$$\#\{r : | r | \leq g(| p |) \} \leq c_0 p^{49+7\alpha+8\beta}.$$

For all $< p, q_1, q_2, q_3 > \in T(p)$ let

$$S(< p, q_1, q_2, q_3 >)$$

$$=$$

$$\left\{ < h_0, h_1, h_2 >: \begin{array}{l} h_0 \in F_p[x] \ \& \ h_1 \in F_{q_1}[x] \ \& \\ h_2 \in F_{q_2}[x] \ \& \ \mathcal{D}(h_0) = q_1 \ \& \\ \mathcal{D}(h_1) = q_2 \ \& \ \mathcal{D}(h_2) = q_3 \end{array} \right\}$$

Where $\mathcal{D}$ is as in section 3.

By Assumption 1 and Theorem 3 there exists a $c_1 \in \mathbf{N}$ such that

$$\#S(< p, q_1, q_2, q_3 >) > p^{38.5}/\log^{c_1}(p).$$

Let

$$W(p) = \bigcup S(< p, q_1, q_2, q_3 >)$$

where the union is over all $< p, q_1, q_2, q_3 > \in T(p)$.

By the previous lemma there exists a $c_2 \in \mathbf{N}$ such that

$$\#W(p) > p^{49}/\log^{c_2}(p).$$

For all $< h_0, h_1, h_2 > \in W(p)$ let

$$R(< h_0, h_1, h_2 >)$$

$$=$$

$$\left\{ r : \begin{array}{l} \mid r \mid \leq g(\mid p \mid) \text{ \& } \textit{algorithm } A \textit{ on input } p, r \\ \textit{calculates } f_0 = h_0 \text{ \& } f_1 = h_1 \text{ \& } \\ f_2 = h_2 \text{ \& } \textit{outputs } 1 \end{array} \right\}$$

By Assumptions 2 and 3 there exists a $c_3 \in \mathbf{N}$ such that

$$\#R(< h_0, h_1, h_2 >) > p^{7\alpha + 8\beta}/c_3$$

Hence, there exist a $c_4 \in \mathbf{N}$ such that

$$\#\{r : \mid r \mid \leq g(\mid p \mid) \text{ \& } f(p, r) = 1\} \geq p^{49+7\alpha+8\beta}/\log^{c_4}(p)$$

as desired. □

5 Assumptions

The following assumptions are used in the previous text. These assumptions will be proved in subsequent papers. For definitions see Section 3.

For all rational primes p,q, let $N_C(p, q)$ denote the number of F_p-isomorphism classes of F_p-curves of genus 2 with q F_p-rational points on the Jacobian.

Assumption 1 *There exist $d, e \in Z_{>0}$ such that for all rational primes p,*

$$\frac{\# \left\{ q : \begin{array}{c} q \textit{ prime} \text{ \& } \\ p^2 - p^{1.5} \leq q \leq p^2 \text{ \& } \\ N_C(p, q) < p^{1.5}/\log^e(p) \end{array} \right\}}{\#\{q : q \textit{ prime} \text{ \& } p^2 - p^{1.5} \leq q \leq p^2\}} < \frac{1}{\log^d(p)}.$$

Assumption 2 *There exist an $\alpha \in \mathbf{N}$ and a polynomial time computable everywhere defined function $\mathcal{G}$: $S \times \mathbf{N} \to \mathbf{N}$ where $S = \{< n, f >: n \in \mathbf{N}$ and $f \in \mathbf{Z}/n\mathbf{Z}[x]$ of degree 6 $\}$ such that:*

1. *For all $< n, f > \in S$ with n prime and f without multiple roots:*

   (a) *for all $r \in \mathbf{N}$, $\mathcal{G}(< n, f >, r) = 0$ or $\mathcal{G}(< n, f >, r) = \mathcal{D}(f)$*

   (b)
   $$\frac{\# \left\{ r : \begin{array}{l} \mid r \mid \leq \mid n \mid^{\alpha} \\ \text{\&} \\ \mathcal{G}(< n, f >, r) = \mathcal{D}(f) \end{array} \right\}}{\#\{r : \mid r \mid \leq \mid n \mid^{\alpha}\}} \geq \frac{1}{2}$$

2. *For all $< n, f > \in S$ with n prime and f with multiple roots, for all $r \in \mathbf{N}$ $\mathcal{G}(< n, f >, r) = 0$.*

3. *For all $< n, f > \in S$ with n composite for all $r \in \mathbf{N}$ $\mathcal{G}(< n, f >, r)$ is not prime.*

This assumption is a generalization of the results of Schoof [S] on elliptic curves.

Assumption 3 *There exist a polynomial time computable everywhere defined function $\mathcal{H} : \mathbf{N}^2 \to \{0, 1\}$, a $c \in \mathbf{R}$ with $c < 15/16$ and a $\beta \in \mathbf{N}$ such that both:*

1. *for all $n \in \mathbf{N}$ with n composite for all $r \in \mathbf{N}$,*

   $$\mathcal{H}(n, r) = 0.$$

2. *for all $x \in \mathbf{N}$ let $\mathcal{E}(x)$ be the set of all rational primes p less than x such that*

   $$\frac{\#\{r \in \mathbf{N} : \mid r \mid \leq \mid p \mid^{\beta} \text{ \& } \mathcal{H}(p, r) = 1\}}{\#\{r : \mid r \mid \leq \mid p \mid^{\beta}\}} < \frac{1}{2},$$

   then $\#\mathcal{E}(x) \leq x^c$.

This assumption is a refinement of the result of Goldwasser and Killian [GK].

6 Remarks

It is possible to recast Theorem 1 in several different forms. Combining Theorem 1 with the result of Solovay and Strassen [SS] yields the following:

Theorem 4 (Assumption 1 through 3 imply) *There exist a $c \in \mathbf{N}$ and a polynomial time computable everywhere defined function $\mathcal{F} : N^2 \rightarrow \{0, 1, ?\}$ such that both:*

1. *for all $n \in \mathbf{N}$ with n composite both:*

   (a) *for all $r \in \mathbf{N}$*

   $$\mathcal{F}(n, r) \neq 1$$

   (b)

   $$\frac{\#\{r : |r| \leq |n|^c \ \& \ \mathcal{F}(n, r) = 0\}}{\#\{r : |r| \leq |n|^c\}} \geq \frac{1}{2}$$

2. *for all $p \in \mathbf{N}$ with p prime both:*

   (a) *for all $r \in \mathbf{N}$*

   $$\mathcal{F}(p, r) \neq 0$$

   (b)

   $$\frac{\#\{r : |r| \leq |p|^c \ \& \ \mathcal{F}(p, r) = 1\}}{\#\{r : |r| \leq |p|^c\}} \geq \frac{1}{2}$$

It is also possible to state the result in terms of "short" proofs of primality and compositeness. Let $\mathcal{L}$ denote the first order language of arithmetic, let $\mathcal{L}^{sent}$ denote the sentences of $\mathcal{L}$, and let $\mathcal{P} \subset \mathcal{L}^{sent}$ be Peano's axioms for arithmetic. Let ϕ be a formula of $\mathcal{L}$ with one free variable which defines the set of primes. For all $n \in \mathbf{N}$ let $\phi(n)$ denote the sentence of $\mathcal{L}$ obtained by substituting n for the free variable in ϕ. For all primes p let $\mathcal{D}(p)$ denote the set of all deductions of $\phi(p)$ from $\mathcal{P}$. For all composites n let $\mathcal{D}(n)$ denote the set of all deductions of $\neg\phi(n)$ from $\mathcal{P}$. Finally, let $\mathcal{D}$ denote the set of all deductions from $\mathcal{P}$.

Theorem 5 (Assumption 1 through 3 imply) *There exists $c \in \mathbf{N}$ and a polynomial time computable everywhere defined function $\mathcal{F} : N^2 \rightarrow \mathcal{D} \cup \{?\}$ such that for all $n \in \mathbf{N}$ both:*

1. *for all $r \in \mathbf{N}$*

   $$\mathcal{F}(n, r) \in \mathcal{D}(n) \cup \{?\}$$

2.

   $$\frac{\#\{r : |r| \leq |n|^c \ \& \ \mathcal{F}(n, r) = ?\}}{\#\{r : |r| \leq |n|^c\}} < \frac{1}{2}$$

Since the function $\mathcal{F}$ is computable in polynomial time the deductions referred to in the theorem are of length polynomial in the length of the number n.

7 Acknowledgement

We wish to thank the many mathematicians and computer scientists who have contributed to this research. David Cantor, Ching Li Chai, Eric Kaltofen, Barry Mazur, Victor Miller, Andrew Odlyzko, Carl Pomerance, Ken Ribet, Rene Schoof, Harold Stark, and William Waterhouse.

We owe special thanks to Mike Fried, Hendrik W. Lenstra Jr., Kevin McCurley, and J. P. Serre.

References

[AH] L.M. Adleman and M.A. Huang, Recognizing Primes in Random Polynomial Time, abstract, 1986.

[APR] L.M. Adleman, C. Pomerance, and R.S. Rumely, On Distinguishing Prime Numbers from Composite Numbers, *Annals of Math.*, 117, (1983), 173-206.

[F] G. Faltings, Endlichkeitssatze fur abelsche Varietaten uber Zahlkorpern, *Invent. Math.* 73 (1983), 349-366.

[G] K.F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, Fleischer, 1801. Translated into English by A.A. Clark, S.J., Yale University Press, New Haven, 1966.

[GK] S. Goldwasser and J. Kilian, Almost All Primes can be Quickly Certified, *Proc. 18th ACM Symp. on Theory of Computing*, pp. 316-329,(1986).

[H] T. Honda, Isogeny Classes of Abelian Varieties Over Finite Fields, *J. Math. Sco. Japan* 20 (1968),83-95.

[IJ] H. Iwaniec and M. Jutila, Primes in Short Intervals, *Ark. Mat.* 17, no. 1, (1979), 167-176.

[L] H.W. Lenstra, Jr., Factoring Integers Using Elliptic Curves Over Finite Fields, Preprint, May 1986.

[M] G. Miller, Riemann Hypothesis and Tests for Primality, *J. Computer and System Science* 13 (1976), 300-317.

[Mu1] D. Mumford, *Abelian Varieties*, Oxford University Press, London, 1970.

[Mu2] D. Mumford, *Tata Lectures of Theta I II*, Progress in Math, V28, Birkhauser, 1983.

[P] V. Pratt, Every Prime Has a Succint Certificate, *Siam J. Computing* 4 (1975), 214-220.

[S] R. Schoof, Elliptic Curves Over Finite Fields and the Computation of Square Roots Mod P, *Math. Comp.* 44, (1985), 483-494.

[SS] R. Solovay and V. Strassen, A Fast Monte-Carlo Test for Primality, *Siam. Jour. Computing* 6 (1977) 84-85.

[ST] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, Publ. Math. Soc. Japan No.6, Tokyo, 1961.

[SeT] J. P. Serre and J. Tate, Good Reduction of Abelian Varieties,*Annals of Math.* 88 (1968) 492-517.

[T] J. Tate, Endomorphisms of Abelian Varieties Over Finite Fields, *Invent. Math.* 2 (1966) 134-141.

[W1] A. Weil, The Field of Definition of a Variety, *Am. Jour. Math.* 78 (1956), 509-524.

[W2] A. Weil, Zum Beweis des Torellischen Satzes, *Nachr. Akad. Wiss. Gottingen, Math. Phys*, K1 (1957) 33-53.

[Wa] W. Waterhouse, Abelian Varieties Over Finite Fields, *Ann. Scient. Ec. Norm. Sup.* 4 (1969) 521-560.