The Extended Riemann Hypothesis and its Application to Computation

Jason Wojciechowski

22nd January 2003

1 Introduction

Many of Hilbert's 23 famous problems are not of a prove or disprove nature; rather, they are open-ended, "of a purely investigative nature," [12] and may never be answered to satisfaction. One of the best examples of this is the sixth problem, that of the axiomatization of physics. Hilbert said, "The investigations on the foundations of geometry suggest the problem: *To treat in the same manner, by means of axioms, those physical sciences in which mathematics plays an important part; in the first rank are the theory of probabilities and mechanics*" [15]. Eight of the 23 problems can be regarded this way, and of the other 15, just three remain unsolved. One of those three, the Riemann Hypothesis, has remained "as mysterious and challenging as ever" [12] and is thus one the Clay Mathematics Institute's seven Millennium Prize Problems.

The purpose of this paper is to survey the uses of the Extended Riemann Hypothesis in creating algorithms to perform various mathematical tasks. We will begin with an introduction to the Riemann Hypothesis and Extended Riemann Hypothesis, then move on to the applications. We will only spend time on proving one of those applications (the Solovay-Strassen primality test, which will be our first topic), but we will also discuss factoring polynomials over finite fields, factoring integers, searching for primitive roots, and finding k^{th} power nonresidues modulo a prime. We will conclude with a brief discussion of why the Extended Riemann Hypothesis might be true.

2 The Riemann Hypothesis

The Riemann Hypothesis can be stated in a number of equivalent forms. Because it also has a number of consequences, the consequences can sometimes be confused with the forms of the hypothesis itself. We will try to avoid such confusion here.

The official Millennium Prize Problem description written by Bombieri [7] gives the hypothesis in the terms of Riemann's zeta-function.

Definition 2.1. *The* **Riemann zeta-function** *is*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

where s is a complex variable and the real part of s is greater than 1.

Note that if $s \leq 1$, $\zeta(s)$ is not convergent. Sondow [24] obtained an analytic continuation (a power series representation of a function whose radius of convergence extends beyond the domain of the original function) of the zeta-function to the whole complex plane (except for a pole at $s = 1$) using Euler's transformation of series. That continuation takes the form

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{-s}.$$

This form of the zeta function has zeros, known as *trivial zeros*, at the negative even integers. However, it also has a number of other zeros. One Riemann Hypothesis, then, is

Riemann Hypothesis 1. *The non-trivial zeros of $\zeta(s)$ have real part equal to $\frac{1}{2}$.*

Riemann's original conjecture was actually about the zeros of a related zeta-function, but it is equivalent to Riemann Hypothesis 1.

Euler showed that the zeta-function can also be expressed as the product over the set of primes

$$\zeta(s) = \prod_{p} \frac{1}{(1 - p^{-s})}.$$

Patterson says that this formulation "is the reason for the significance of the zeta-function." A proof that the two expressions of the zeta functions are equivalent can be found in Patterson's book [18].

The above representation of the zeta-function is our first suggestion that the Riemann Hypothesis might have consequences in number theory, and indeed there is a more purely number theoretic form of the hypothesis. Before we give that form, though, we need a definition.

Definition 2.2. *The* **logarithmic integral** $li(x)$ *is defined as*

$$li(x) = \int_2^x \frac{dt}{\log t}.$$

Recalling that $\pi(x)$ is the number of primes less than x, we have

Riemann Hypothesis 2.

$$\pi(x) = li(x) + \mathcal{O}(x^{1/2+\epsilon}).$$

Finally, we can state two more equivalent hypotheses, also about prime numbers. We need two new functions, the Chebyshev ψ and ϑ functions.

Definition 2.3.

$$\psi(x) = \sum_{p^k \leq x} \log p = \log(lcm(1, 2, 3, \ldots, \lfloor x \rfloor)),$$

summing over all primes p and all non-negative integers k.

Now, we have the third formulation.

Riemann Hypothesis 3. $\forall \epsilon > 0$,

$$\psi(x) = x + \mathcal{O}(x^{1/2+\epsilon}).$$

Finally, we define the Chebyshev ϑ function as

Definition 2.4.

$$\vartheta(x) = \sum_{p \leq x} \log p.$$

and give our final statement of the Riemann Hypothesis.

Riemann Hypothesis 4. $\forall \epsilon > 0$,

$$\vartheta(x) = x + \mathcal{O}(x^{1/2+\epsilon}).$$

All of the above is as given in [5].

3 The Extended Riemann Hypothesis

The evidence from the last three Riemann Hypotheses that it is going to be of use in number theoretic (and perhaps computational number theoretic) problems leads us to the Extended Riemann Hypothesis (ERH). As with the original Riemann Hypothesis, we find a number of formulations of the ERH.

Chowla [11] first defines a function L_p of a complex variable s:

$$L_p(s) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \frac{1}{n^s},$$

where $\left(\frac{n}{p}\right)$ is the *Legendre Symbol*, defined for p prime as

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p|n \\ 1 & \text{if } n \text{ is a quadratic residue mod } p \text{ and } p \not| n \\ -1 & \text{if } n \text{ is a quadratic nonresidue mod } p \text{ and } p \not| n. \end{cases}$$

The ERH, then, is:

Extended Riemann Hypothesis 1. *All the zeros of $L_p(s)$ which lie in the "critical strip" (zeros with real part strictly between 0 and 1) have real part equal to $\frac{1}{2}$.*

The ERH can also be set out this way, as in [5]:

Extended Riemann Hypothesis 2. *For n and a relatively prime integers and $\epsilon > 0$,*

$$\pi(x, n, a) = \frac{li(x)}{\phi(n)} + \mathcal{O}(x^{1/2+\epsilon}).$$

$\pi(x, n, a)$ here is the number of primes less than or equal to x and equivalent to a mod n.

This version recalls Riemann Hypothesis 2, especially in the absence of functions of complex variables, zeta functions, L-functions, or anything of that sort.

To give one final definition of the ERH, we first define a character.

Definition 3.1. *A* **character** *on a finite Abelian group G is a homomorphism (a map that preserves the group operation) from G to the unit circle.*

Let μ be a character on $\mathbb{Z}_n^*$. We define the **Dirichlet character** χ *as*

$$\chi(m) = \begin{cases} \chi(m \bmod n) & \text{if } gcd(m,n) = 1 \\ 0 & \text{otherwise} \end{cases}$$

If χ is always 0 or 1, it is called **principal**.

This leads, then, to

Extended Riemann Hypothesis 3. *[5] Define the* **Dirichlet** L**-function** *to be*

$$L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

when the real part of $s > 1$ and, as before, analytic continuation otherwise. $L(s,\chi)$ has infinitely many zeroes in $0 < \Re(s) < 1$. The ERH, then, is that all zeros in that interval have real part $\frac{1}{2}$.

This is obviously very similar to Extended Riemann Hypothesis 1 above; the only difference lies in how the L function is stated.

When we discuss numerical evidence for the ERH later, this is the form we will refer to.

Bach and Shallit [5] note that the "'extended' or 'generalized' Riemann hypothesis is interpreted differently by different authors" and quote Narkiewicz [16] to give a general overview of how the ERH should be seen: "We use ERH ... to denote the statement that every conceivable zeta-function which should not have zeroes in the critical strip indeed does not have them."

4 Solovay-Strassen primality test

In 1977, Solovay and Strassen [23] published a Monte-Carlo algorithm (the first randomized algorithm, actually) for testing primality which can be derandomized under the Extended Riemann Hypothesis. The algorithm proceeds as follows:

```
input odd integer n ≥ 3
pick a randomly from (1, 2, 3, ..., n − 1)
if gcd(a, n) = 1:
      if (a/n) ≡ a^((n−1)/2) (mod n):
          return prime
else:
```

```
return composite
```

Then we have as a first goal for this section the following theorem (where the true goal is to show that we don't need the randomness in the algorithm).

Theorem 4.1. *If n is prime, the Solovay Strassen test returns prime. If n is composite, it returns composite for at least $1/2$ of the a's in $(1, 2, 3, \ldots, n-1)$. The algorithm runs in polynomial time.*

Thus the Solovay-Strassen algorithm actually gives a certificate for compositeness, rather than primality.

We will need a few tools to carry out the proof of this theorem.

First, recall that the Legendre symbol was only defined for n prime, but we may have n composite in the algorithm. Jacobi generalized the Legendre symbol to all odd integers, regardless of primality.

Definition 4.2 (Jacobi Symbol). *Let n be odd with prime factorization $\prod p_i^{e_i}$. Then*

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)$$

where the symbol in the product is the Legendre symbol.

Next we pick up Euler's Criterion.

Lemma 4.3 (Euler's Criterion). *Let p be an odd prime and let a be an integer such that $gcd(a, p) = 1$. Then a is a quadratic residue mod p if $a^{(p-1)/2} \equiv 1 \pmod{p}$ and a is a nonresidue if $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Proof. Let $x = a^{(p-1)/2}$. Then

$$x^2 = a^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem, so $x = \pm 1$.

Suppose there exists b such that $b^2 \equiv a \pmod{p}$. Then we have

$$x = a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}$$

where we again apply Fermat's Little Theorem at the end.

Now suppose that a is a nonresidue mod p. Since there are at most $\frac{p-1}{2}$ roots of the equivalence $z^{(p-1)/2} \equiv 1 \pmod{p}$ and there are $\frac{p-1}{2}$ quadratic residues mod p (since p is an odd prime), the only roots of the equivalence are the quadratic residues mod p. Since a is not one of those, but $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$, a must be $-1 \pmod{p}$. □

Definition 4.4. *The group of* **Euler liars** $E(n)$ *is defined*

$$E(n) = \{a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}\},$$

where $\mathbb{Z}_n^*$ is the group of integers relatively prime to n, also known as the group of units of the field $\mathbb{Z}_n$.

This group can be illustrated with the analogy "Euler liars are to Euler's Criterion as Carmichael numbers are to Fermat's Little Theorem[1]."

Lemma 4.5. *Let n be an odd integer ≥ 3. Then n is prime if and only if $E(n) = \mathbb{Z}_n^*$.*

To prove this, we'll need some facts about Carmichael numbers, as well as a new function.

Definition 4.6. *The* **Carmichael lambda function** $\lambda(n)$ *denotes the least positive exponent c such that $a^c \equiv 1 \pmod{n}$ for all a in $\mathbb{Z}_n^*$.*

So we can now state the next lemma.

Lemma 4.7. *A composite number n is Carmichael if and only if $\lambda(n)|(n-1)$.*

Proof. If n is Carmichael, then $a^{(n-1)} \equiv 1 \pmod{n}$ for any appropriate a. Any c such that $a^c \equiv 1 \pmod{n}$, then, must be a factor of $(n-1)$.

Now suppose $\lambda(n)|(n-1)$. Since $a^{\lambda(n)} \equiv 1 \mod n$ for all appropriate a, $a^{k\lambda(n)} \equiv 1 \pmod{n}$ for all k. Since multiplication with one of those k's results in $(n-1)$, we have $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^*$, so a is Carmichael. □

[1]Carmichael numbers are composite n such that, for all $a < n$, with $\gcd(a, n) = 1$, we have $a^{n-1} \equiv 1 \pmod{n}$.

We state without proof the following facts about $\lambda(n)$. Proof can be found in [5].

Lemma 4.8. *The following are properties of* $\lambda(n)$*:*

1. $\lambda(1) = 1$,
2. $\lambda(p^e) = p^{c-1}(p-1)$ *if* p *is an odd prime,*
3. $\lambda(2) = 1, \lambda(4) = 2, \lambda(2^c) = 2^{c-2}$ *for* $c > 2$,
4. *if* n *is a product of prime powers* $\prod p_i^{c_i}$*, then* $\lambda(n) = lcm(\lambda(p_i^{c_i}))$.

We require just one last result before we can prove Lemma 4.5.

Lemma 4.9. *If* n *is a Carmichael number, then it is square free.*

Proof. First we show that n must be odd. Suppose that n has an odd factor. Then $\lambda(n)$ will have an even factor, due to the second and fourth parts of Lemma 4.8. If n has no odd factor, then part three of Lemma 4.8 shows that $\lambda(n)$ has an even factor. Thus $2|\lambda(n)$, so by Lemma 4.7, $(n-1)$ is even, so n is odd.

To prove that n is squarefree, suppose for a contradiction that $p^2|n$, where p is a prime. Since n is odd, p is odd, so one of $\lambda(n)$'s factors is $p(p-1)$. Thus $p|\lambda(n)$ and so by Lemma 4.7, $p|(n-1)$. Since $p|n$ and $p|(n-1)$, $p|1$, so $p = 1$, but p is prime, so we have reached a contradiction. □

Thus we can now carry out the following proof.

Proof of Lemma 4.5. Assume $E(n) = \mathbb{Z}_n^*$, but suppose that n is composite. Then

$$a^{n-1} = (a^{(n-1)/2})^2 \equiv \left(\frac{a}{n}\right)^2 \equiv (\pm 1)^2 \equiv 1 \pmod{n},$$

where the second to last equivalence is true because $\gcd(a, n) = 1$. Then n is Carmichael, so by Lemma 4.9, it is squarefree. We write $n = pr$, where p is prime and $\gcd(r, p) = 1$.

Let g be a quadratic residue mod p and let $a \equiv g \pmod{p}$ and $a \equiv 1 \pmod{r}$. Then we have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{pr}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{r}\right) = \left(\frac{g}{p}\right)\left(\frac{1}{r}\right)$$

where the last equality is true because a quadratic residue can only be congruent to another quadratic residue, and similarly for nonresidues.

We defined g to be a nonresidue mod p and 1 is clearly a residue to any modulus, so we are left with

$$\left(\frac{g}{p}\right)\left(\frac{1}{r}\right) = (-1)(1) = -1.$$

Since we assumed that $\left(\frac{a}{n}\right) = a^{(n-1)/2}$, we have $a^{(n-1)/2} \equiv -1 \pmod{n}$, so $r|n$ implies that $a^{(n-1)/2} \equiv -1 \pmod{r}$, but that contradicts $a \equiv 1 \pmod{r}$ unless $r = 2$, but r cannot be 2, because n is odd. □

And thus we have reached our (intermediary) goal, the proof of the correctness of the Solovay-Strassen algorithm.

Proof of Theorem 4.1. If n is prime, the first `if` test will be passed regardless of the choice of a and the second `if` test will be passed by Euler's Criterion, so "prime" will be returned.

Otherwise, we have either $n \in \mathbb{Z}_n^*$ or not. If n is not in the group, then it will fail the first `if` statement and "composite" will be returned.

So suppose that n is in the group. We know from Lemma 4.5 that $E(n) \neq \mathbb{Z}_n^*$, but $E(n)$ is clearly a subgroup of $\mathbb{Z}_n^*$, so it is a proper subgroup, giving us

$$|E(n)| \leq \frac{|\,\mathbb{Z}_n^*\,|}{2} = \frac{\phi(n)}{2} \leq \frac{(n-1)}{2} \leq \frac{n}{2},$$

where the first inequality is true because the order of a subgroup must divide the order of the group. Thus the size of the group of Euler liars, which is the size of the set of false positives given by the algorithm, is less than half the size of the set, as required.

It is well known that the greatest common divisor can be computed in polynomial time. Proof that the Jacobi symbol and $a^{(n-1)/2} \pmod{n}$ can be computed in polynomial time can be found in [5]. □

Thus we have a working primality test that runs in polynomial time. Really, though, since we have an algorithm that always returns prime if n is prime and more than half the time returns composite

if n is composite, it would be more accurate to call the Solovay Strassen test a "compositeness test," at least for the purposes of stating that it is in the complexity class **RP** (randomized polynomial time).

Agrawal, Kayal, and Saxena [1] recently proved that primality testing is unconditionally in **P**. Before then, however, all deterministic polynomial-time primality tests depended on the ERH. The Solovay Strassen test can be derandomized to obtain such a conditional algorithm.

The derandomized algorithm is:

```
input odd integer n ≥ 3
for a = 2 to 2(log n)^2:
      if gcd(a, n) ≠ 1:
          return 'composite'
      else if (a/n) ≢ a^((n-1)/2) (mod n):
          return 'composite'
return 'prime'
```

First note that the only real difference between the deterministic and random versions is the use of a `for` loop to touch all a up to $2(\log n)^2$ instead of randomly choosing an a.

To prove the correctness of this algorithm, we must define another function, $\Lambda(n)$ and state a lemma.

Definition 4.10. *The* **von Mangoldt lambda function** $\Lambda(n)$ *is defined*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \\ 0 & \text{otherwise.} \end{cases}$$

Next, for convenience, set $G(n) = \min\{x : \mathbb{Z}_n^* \text{ is generated by primes} \leq x\}$.

Proof of the following lemma can be found in [5].

Lemma 4.11. *Assume the ERH. Let χ be a Dirichlet character, and let $1_\chi = 1$ when χ is principal and 0 otherwise. Then*

$$\sum_{p \leq x} \Lambda(p)\chi(p)(x-p) = 1_\chi \frac{x^2}{2} + \mathcal{O}(x^{3/2} \log n).$$

Now, we get to a rather important result due to Ankeny. The theorem is important enough to applications of the ERH that Weisstein's MathWorld entry for the ERH [27] is essentially this theorem.

Theorem 4.12 (Ankeny's Theorem). *Assume the ERH. Then* $G(n) = \mathcal{O}((\log n)^2)$ *and every nontrivial subgroup of* $\mathbb{Z}_n^*$ *omits a positive number* $a = \mathcal{O}((\log n)^2)$.

Ankeny's original formulation [2] states the theorem in its more commonly quoted form: the first quadratic nonresidue mod p is $\mathcal{O}((\log p)^2)$. In fact, this can be sharpened to say that the least quadratic nonresidue mod p is less than or equal to $2(\log p)^2$, as in the theorem as stated above.

Proof. First note that if $x > 0$ and the p's are those primes less than or equal to x mentioned in the definition of $G(n)$,

$$\begin{aligned}\sum_{\substack{p\le x\\ p|n}} \Lambda(p)(x-p) &= \sum \log p(x-p)\\ &= x\sum \log p - \sum p\log p\\ &= x\log(\prod p) - \sum p\log p\\ &\le x\log n - \sum p\log p\\ &\le x\log n.\end{aligned}$$

Now assume that the primes less than or equal to x do not generate $\mathbb{Z}_n^*$. Then they generate a proper subgroup of $\mathbb{Z}_n^*$, so we can choose a nonprincipal Dirichlet character χ such that $\chi(n)$ is 0 or 1 for all $n < x$. Then, since χ is nonprincipal, by Lemma 4.11, we have

$$\sum_{p\le x} \Lambda(p)\chi(p)(x-p) = \mathcal{O}(x^{3/2}\log n).$$

Now,

$$\sum_{p\le x} \Lambda(p)\chi(p)(x-p) = \sum_{p\le x}(x-p)\log p - \sum_{\substack{p\le x\\ p|n}} \Lambda(p)(x-p)$$

since $\chi(p) = 0$ when $p|n$. The first term of the right hand side can be rewritten as before as

$$x \sum_{p \leq x} \log p - \sum_{p \leq x} p \log p.$$

The first term of the new expression then becomes $x\vartheta(x)$, where $\vartheta(x)$ is the Chebyshev function defined above. But $\vartheta(x) \sim x$ [5]. Since a consequence of the prime number theorem is that the p^{th} prime is about $p \log p$, the second term gives

$$\sum_{p \leq x} p \log p \sim \sum_{n \leq x} n \sim \frac{x^2}{2}.$$

All together, then, the first term of the right hand side of the original expression is $\Omega(x^2)$. Combining with the estimate obtained for the second term above, we see that the whole expression is $\Omega(x^2 - x \log n)$.

Thus,

$$\begin{aligned}
\Omega(x^2 - x \log n) &= \mathcal{O}(x^{3/2} \log n) \\
x^2 - x \log n &= \mathcal{O}(\mathcal{O}(x^{3/2} \log n)) \\
x^2 - x \log n &= \mathcal{O}(x^{3/2} \log n) \\
x^{1/2} - \frac{\log n}{x^{1/2}} &= \mathcal{O}(\log n) \\
\sqrt{x} &= \mathcal{O}(\log n) + \frac{1}{\sqrt{x}} \log n \\
\sqrt{x} &\leq c \log n + \frac{1}{\sqrt{x}} \log n \\
\sqrt{x} &\leq (c + \frac{1}{\sqrt{x}}) \log n \\
\sqrt{x} &= \mathcal{O}(\log n) \\
x &= \mathcal{O}((\log n)^2)
\end{aligned}$$

and the proof is complete, since $G(n)$ must be less than this x by our assumption on x, thus $G(n)$ is also $\mathcal{O}((\log n)^2)$. □

Ankeny's Theorem lets us prove the next theorem, after which we will be able to reach our ultimate goal for this section.

Theorem 4.13. *Assume the ERH. If n is an odd composite integer, then there is a positive integer $a < n$ with $a \leq 2(\log n)^2$ for which either $gcd(a, n) \neq 1$ or $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \pmod{n}$.*

Proof. By Lemma 4.5, $E(n)$ is a proper nontrivial subgroup of $(\mathbb{Z}(n))^*$ when n is an odd composite integer. By Ankeny's Theorem, there is an $a = \mathcal{O}((\log n)^2)$ in $\mathbb{Z}_n - E(n)$, since the complement of $\mathbb{Z}_n - E(n)$ is a nontrivial subgroup of $\mathbb{Z}_n^*$. If $a \notin \mathbb{Z}_n^*$, then $\gcd(a, n) \neq 1$; if $a \in \mathbb{Z}_n^*$, then $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$, since a is not in $E(n)$. □

We now have the tools to prove the correctness of the deterministic version of the Solovay-Strassen algorithm.

Theorem 4.14. *Assuming the ERH, the deterministic Solovay-Strassen algorithm returns prime if and only if n is prime, and does so in polynomial time.*

Proof. By Theorem 4.13, if n is composite, one of the two `if` tests will return composite, so if neither test is ever passed n must be prime.

Since we only test $2(\log n)^2$ values of a at most, the polynomial running time follows from the fact that the original algorithm ran in polynomial time (since this algorithm uses only the computations the original one did). □

5 Primitive roots in finite fields

Though the Riemann Hypothesis is stated in terms of a complex function, it is, as Papadimitriou says in [17], "a most important *number-theoretic conjecture* concerning the roots of the Riemann ζ function and *the distribution of primes*" (emphasis added). That said, not all problems that make use of the Riemann Hypothesis are strictly number theoretic. Shoup [22] showed in 1992 that, assuming the Extended Riemann Hypothesis, there is a deterministic polynomial time search procedure for finding a primitive root in a specific finite field (though there is no known procedure for general finite fields).

The idea of primitive roots is not strictly "un-number theoretic," of course, but Shoup defines them in terms of finite fields rather than simply as numbers modulo other numbers, lending the result a more algebraic flavor.

Definition 5.1. *In a finite field $\mathbf{F}_{p^n}$ where p is prime and n is a positive integer, a nonzero element $g \in \mathbf{F}_{p^n}$ is called a* **primitive root** *if it generates $\mathbf{F}_{p^n}^*$, the group of units of $\mathbf{F}_{p^n}$.*

Shoup notes that since there are no known polynomial time algorithms for generating primitive roots, or even for testing whether a given element is a primitive root, we resort instead to the aforementioned "search procedures." A search procedure is an algorithm that generates a subset of the finite field that contains at least one primitive root. In the case of a randomized algorithm, this would mean that the subset generated had a high probability of containing a primitive root.

Finally, we state the aforementioned theorem.

Theorem 5.2. *Assume the ERH. Then there is a deterministic polynomial-time search procedure for primitive roots in $\mathbf{F}_{p^2}$.*

The proof of the theorem actually shows that a field $\mathbf{F}_p(\alpha)$ isomorphic to $\mathbf{F}_{p^2}$ can be constructed in polynomial time such that $\exists(a + b\alpha) \in \mathbf{F}_p(\alpha)$, where $(a + b\alpha)$ is a primitive root with $a, b \in \mathbb{Z}$ and the absolute values of a and b are both $(\log p)^{\mathcal{O}(1)}$. This proof depends on a theorem due to Lenstra [14] which says that a field isomorphic to $\mathbf{F}_{p^2}$ can be constructed in polynomial time assuming the ERH. The details of the proof can be found in [22].

Shoup notes that his "proof of this theorem does not generalize to arbitrary finite fields $\mathbf{F}_{p^n}$, even for fixed $n > 2$."

6 The least primitive root modulo p, a large prime

Alternatively, we can define primitive roots without mentioning fields explicitly. Rosen [19] defines them this way:

Definition 6.1. *If r and n are relatively primes integers with $n > 0$ and if $ord_n r = \phi(n)$, then r is called a* **primitive root modulo n**.

Recall that the order of an integer $r \pmod n$ is the least positive x such that $r^x \equiv 1 \pmod n$ and $\phi(n)$ denotes the number of integers less than n which are relatively prime to n.

Shoup and Bach both cite a result of Wang [26] which shows that there is a primitive root $x \pmod p$ with $x = (\log p)^{\mathcal{O}(1)}$, or, more

precisely, $x = \mathcal{O}(r^6(\log p)^2)$, where $r = \omega(p-1)$, the number of distinct prime divisors of $p-1$.

Shoup [22], using the same basic methods that he used to prove Theorem 5.2, proved the following theorem.

Theorem 6.2. *Assume the ERH. Then the least primitive root modulo p is $\mathcal{O}(r^4(\log r+1)^4(\log p)^2)$, where r is as above.*

This bound simplifies to $\mathcal{O}((\log p)^6)$. This result implies the ability to construct a set S such that a primitive root mod p is in S. Bach gives a method in [3], however, that constructs a smaller set (albeit one with larger numbers) than Shoup's, and does so using simpler methods which allow the statement of an explicit algorithm. We give that algorithm now.

Input odd prime p
Find $B \geq 1$ so that $B \log B = 30 \log p$
Factor $p-1 = Q\prod q_i^{e_i}$ where $q_i < B$
    and Q is free of primes $< B$
For $i = 1$ to r:
    Choose a prime $b_i \leq 2(\log p)^2$ so that $b_i^{(p-1)/q_i} \not\equiv 1$
    Let $a_i \equiv b_i^{(p-1)/q_i^{e_i}} \pmod p$
Let $a = \prod_{i=1}^{r} a_i$
Let $S = \{ab^{(p-1)/Q} \pmod p : b \text{ is prime and } b \leq 5\frac{(\log p)^4}{(\log\log p)^2}\}$.

Bach proves that

- The algorithm works (i.e. S contains a primitive root mod p);
- The size of the set S is $\mathcal{O}(\frac{(\log p)^4}{(\log\log p)^3})$;
- The running time of the algorithm is $\mathcal{O}(\frac{(\log p)^7}{(\log\log p)^3})$;

but we omit the proof here.

7 Factoring polynomials (and primitive roots return again)

Consider the problem of factoring polynomials of degree less than n over fields with 2^{n^2} or fewer elements. Call this $\texttt{FACTOR}_n$. Then the

more general FACTOR is the family of problems obtained by combining the $\texttt{FACTOR}_n$'s for all $n \in \mathbb{N}$.

Now consider the problem of finding a primitive root (not necessarily the least primitive root, as above, but *any* primitive root) modulo a prime p where $p < 2^n$ and the greatest prime factor of $(p-1)$ is less than or equal to n. Denote this $\texttt{PRIMITIVE}_n$, and let PRIMITIVE be analogous to FACTOR above.

Von zur Gathen [25] showed in 1987 that PRIMITIVE and FACTOR each have polynomial-time reductions to each other; in other words, they are polynomial-time equivalent. More importantly to us, he showed that, under the ERH, FACTOR and PRIMITIVE are in **P**. Note that despite removing the restriction on the size of the field/modulus, this result is compatible with Shoup's statement noted above (that the best we can do for finding primitive roots in general is by using search procedures) as we are only considering p's with $(p-1)$ smooth (i.e. $(p-1)$ only has small prime factors).

Von zur Gathen's result runs in $S(p-1)(n \log p)^{\mathcal{O}(1)}$, where $S(n)$ is the largest prime number dividing n. Shoup [21] improved that running time in the power of its first factor, giving an algorithm that runs in $S(p-1)^{1/2}(n \log p)^{\mathcal{O}(1)}$. Cheng and Huang [10] also give an interesting algorithm based on a combinatorial problem[2]. Their algorithm has $(n^{\log n} \log p)^{\mathcal{O}(1)}$ running time, though it is actually polynomial on average. Also, they note, a combinatorial conjecture would allow them to decrease the exponent of n, giving $(n^{\log \log n} \log p)^{\mathcal{O}(1)}$ worst-case running time.

Perhaps surpassing all of this, however, is Gao's [13] recent proof that, under the ERH, we can factor a polynomial $f \in \mathbf{F}_p[x]$ so long as f does not satisfy a condition he calls being "c-super square balanced." Let us define what this means.

Definition 7.1. *Let $F \subset \mathbf{F}_q, |F| = n > 1$, where $q = p^k$ for some prime p and $k \in \mathbb{Z}^+$. F is* **square balanced** *if, $\forall \xi \in F$,*

$$|\{\zeta \in F : \zeta \neq \xi, \xi - \zeta \text{ is a square in } \mathbf{F}_q\}| = \frac{n-1}{2}.$$

Two sets F_1 and F_2, subsets of $\mathbf{F}_q$ with cardinality greater than 1, are **mutually square balanced** *if, $\forall \xi \in F_1$,*

$$|\{\zeta \in F_2 : \zeta - \xi \text{ is a square in } \mathbf{F}_q\}|$$

[2]The problem is that of finding a stable coloring of tournaments. We will avoid digressing further than this.

is the same for all $\xi \in F_1$, and analogously for all $\xi \in F_2$ with $\zeta \in F_1$.

Next, for a subset F of $\mathbf{F}_q$ and $k \in \mathbb{Z}$, we define $F_k = \{a^k : a \in F\}$. In other words F_k is just the set of k^{th} powers of the elements of F.

Let $c > 1$ be a constant. Then we call F **c-super square balanced** *if each of the following are true:*

1. *$\forall k \in \{1, 2, \ldots, (n \log q)^c\}$, we have F_k square balanced and $|F_k| = n$.*
2. *$\forall k \in \{1, 2, \ldots, (n \log q)^c\}$, the sets F_k are pairwise disjoint.*
3. *$\forall k \in \{1, 2, \ldots, (n \log q)^c\}$, the sets F_k are pairwise mutually square balanced.*

Finally, a polynomial $f \in \mathbf{F}_q[x]$ is **c-super square balanced** *if its set of roots in $\mathbf{F}_q$ is c-super square balanced.*

The above appears to just be another complication, a condition to be met so that Gao's algorithm ends up being just another special case. However, the condition certainly does look strict. Strict enough, in fact, that Gao conjectures the following:

Conjecture 7.2. *For any prime p and any integer $n > 1$, there are no super square balanced subsets in $\mathbf{F}_p$ of cardinality n.*

If this conjecture were true, then, we would have a proof that factoring polynomials over finite fields $\mathbf{F}_p$ was in $\mathbf{P}$, conditional only on the ERH.

Unfortunately, the finite fields $\mathbf{F}_p$ cover only a small portion of the set of all finite fields, so perhaps we are stuck with a special case after all. Fortunately, Berlekamp [6] proved that factoring over any finite field with a prime power number of elements is polynomial-time reducible to factoring over a finite field with a prime number of elements. Thus we can revise the above statement to read, "If this conjecture were true, then, we would have a proof that factoring polynomials over any finite field was in $\mathbf{P}$, conditional only on the ERH."

8 k^{th} power nonresidues

Buchmann and Shoup [9] proved (conditionally on the ERH, of course) that finding k^{th} power nonresidues in a finite field is in **P**. Their theorem is actually stated in terms of finding a generating set for the group of units of a finite field:

Theorem 8.1. *There exists a deterministic algorithm which takes a prime p and a positive integer n and returns a set $S \subset F_{p^n}^*$. Under the ERH, S generates $F_{p^n}^*$.*

It is not immediately obvious how this theorem is useful, but the authors list three consequences of their result, two of which we will mention here.

First is factoring polynomials over F_p. We have already seen that factoring is conditionally in **P**, while this result (which came before Gao's) is unconditional (except on the ERH). Unfortunately, it does not show that factoring polynomials is in **P**. The time an algorithm based on the above theorem would take is a polynomial in the input size times $\sqrt{k}$, where k is the largest prime which divides $\Phi_n(p)$, with Φ_n the n^{th} cyclotomic polynomial. Because

$$\Phi_n(p) = \prod_{k=1}^{n}(p - \zeta_k)$$

where the ζ_k are the primitive roots of unity, $\Phi_n(p)$ could, if n is an odd prime for example, be an $(n-1)$ degree polynomial. Since the k follows from this, we lose the possibility of polynomial time.

The second consequence is the construction of primitive roots in F_{p^n}. However, this result again does not defy Shoup's statement above: the prime factorization of $p^n - 1$ is required in order to obtain a primitive root in deterministic polynomial time.

While both consequences carry strong caveats, they are still noteworthy as they generalize to all n statements that had only previously been proven for $n = 1$ and $n = 2$.

9 Factorization of integers

The problem of factoring integers has garnered widespread interested in the past 30 years, since the introduction of public-key cryptography systems like RSA and the still-growing need for strong

cryptography to aid electronic business transactions have provided practical applications as motivation to pursue this very difficult area of mathematics. Unfortunately (or perhaps fortunately, for those who like online shopping), the ERH does not seem to bring the kinds of results to factoring that it brings to so many other areas.

Seysen [20] created an algorithm in 1987 that ran in

$$e^{\sqrt{\log N \log\log N}\sqrt{5/4}+\mathcal{O}(1)}$$

time and depended on the ERH. This is, of course, not polynomial. Interestingly enough, the algorithm is also not deterministic: rather, it is a Las Vegas algorithm, falling in the complexity class **ZPP**. On input N, the algorithm returns a complete factorization with probability $\frac{1}{2}$, and returns 'prime' for all prime N.

Bach and Shallit [4], not long after Seysen's work appeared, published their own algorithm depending on the ERH which runs in polynomial time, albeit also random. This time, however, there was the requirement that a multiple of $\Phi_k(p)$ be given in order to remove a factor p from the input N. To be fair to the authors, the point of the paper was not to provide a practical algorithm, but to "give a universal construction based on algebraic number theory that subsumes" many of the previous results [4].

That the ERH does so little for pushing integer factoring toward **P** can be a little surprising after spending time watching the hypothesis work magic in so many other areas. Then again, factoring is probably the hardest problem discussed in this paper (after all, how many of the other problems have cryptosystems based on them?), so perhaps it should not be that surprising after all. In fact, we could see the fact of the ERH's relatively minor benefit as further evidence that factoring might remain a "hard" problem.

10 Evidence for the ERH

If the ERH were to be proven false, all of the above results would be rendered false, as well as much other work, in the area of computation as well as outside it. That mathematicians spend time working on algorithms and other pieces of mathematics that depend on the ERH indicates that they believe it, despite the current lack of proof. A fair amount of evidence does in fact exist in favor of the Extended Riemann Hypothesis.

Perhaps more fanfare is given to the empirical evidence for the Riemann Hypothesis, such as that all zeros between $10^{12} + 1$ and $10^{12} + 10^5$ satisfy the hypothesis, or that $2/5$ of the zeros must do the same, but similar evidence exists for the ERH.

Bach and Shallit [5] cite the computational work of over a half dozen researchers, none of whom found any evidence against the ERH. Systematic computations have checked the ERH for the first $10,000$ zeros for all moduli (in the Dirichlet character) less than 14, the first $2,500$ for moduli less than 73, and various others. Others did non-systematic checks and found the same results.

Maybe better (and certainly more interesting) evidence is given by Bombieri [8] (as quoted in [5]), who showed that the maximum error in $\pi(x, n, a) \approx li(x)/\phi(n)$ is bounded by $x^{1/2+\mathcal{O}(1)}$, averaging over all moduli less than or equal to N and letting $x = N^{2+\mathcal{O}(1)}$. In other words, the ERH can be said to be "true on average."

11 Conclusion

Bombieri, in the official problem description of the Riemann Hypothesis for the Clay Mathematics Institute [7] gives one other piece of evidence: "Many deep results in number theory which are consequences of a general Riemann hypothesis can be shown to hold independently of it, thus adding considerable weight to the validity of the conjecture." There are those who still believe that the Riemann Hypothesis is false, but even without the evidence given above, hopeful optimism would probably keep some people going; were the ERH to fall, a lot of mathematics would go with it.

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, *PRIMES is in P*, Available at http://www.cse.iitk.ac.in/news/primality.ps.

[2] N.C. Ankeny, *The least quadratic non residue*, The Annals of Mathematics **55** (1952), no. 1, 65–72.

[3] Eric Bach, *Comments on search procedures for primitive roots*, Mathematics of Computation **66** (1997), no. 220, 1719–1727.

[4] Eric Bach and Jeffrey Shallit, *Factoring with cyclotomic polynomials*, Mathematics of Computation **52** (1989), no. 185, 201–219.

[5] ———, *Algorithmic Number Theory*, Foundations of Computing, vol. 1: Efficient Algorithms, The MIT Press, 1996.

[6] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Mathematics of Computation **24** (1970), no. 111, 713–735.

[7] E. Bombieri, *Problems of the Millenium: the Riemann Hypothesis*, http://www.claymath.org/prizeproblems/riemann.pdf.

[8] ———, *On the large sieve*, Mathematika **12** (1965), 201–225.

[9] Johannes Buchmann and Victor Shoup, *Constructing nonresidues in finite fields and the Extended Riemann Hypothesis*, Mathematics of Computation **65** (1996), no. 215, 1311–1326.

[10] Qi Cheng and Ming-Deh A. Huang, *Factoring polynomials over finite fields and stable colorings of tournaments*, Algorithmic Number Theory (Wieb Bosma, ed.), Lecture Notes in Computer Science, vol. 1838, Springer, July 2000, pp. 233–245.

[11] S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Gordon and Breach, 150 Fifth Ave., New York, NY, 10011, 1965.

[12] *Historical Context, Millenium Prize Problems, Clay Mathematics Institute*, http://www.claymath.org/prizeproblems/history.htm, Accessed 11/30/02.

[13] Shuhong Gao, *On the deterministic complexity of factoring polynomials*, Journal of Symbolic Computation **31** (2001), 19–36.

[14] H.W. Lenstra Jr, *Finding isomorphisms between finite fields*, Mathematics of Computation **56** (1991), no. 193, 329–347.

[15] *Mathematical Problems by David Hilbert*, http://babbage.clarku.edu/~djoyce/hilbert/problems.html, Accessed 11/30/02.

[16] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, 1990.

[17] Christos H. Papadimitriou, *Computational complexity*, Addison-Wesley, 1994.

[18] S. J. Patterson, *An Introduction to the Theory of the Riemann Zeta-Function*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1988.

[19] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, 4th ed., Addison Wesley Longman, 2000.

[20] Martin Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Mathematics of Computation **48** (1987), no. 178, 757–780.

[21] Victor Shoup, *Smoothness and factoring polynomials over finite fields*, Information Processing Letters **38** (1991), 39–42.

[22] ———, *Searching for primitive roots in finite fields*, Mathematics of Computation **58** (1992), no. 197, 369–380.

[23] R. Solovay and V. Strassen, *A fast monte-carlo test for primality*, SIAM Journal of Computing **6** (1977), no. 1, 84–85.

[24] Jonathon Sondow, *Analytic continuation of Riemann's zeta function and values at negative integers via Euler's transformation of series*, Proceedings of the American Mathematical Society **120** (1994), no. 2, 421–424.

[25] Joachim von zur Gathen, *Factoring polynomials and primitive elements for special primes*, Theoretical Computer Science **52** (1987), 77–89.

[26] Y. Wang, *On the least primitive root of a prime*, Scientia Sinica **10** (1961), 1–14.

[27] Eric W. Weisstein, *Extended Riemann Hypothesis*, http://mathworld.wolfram.com/ExtendedRiemannHypothesis.html, Accessed 12/2/02.