Honors 1: Undergraduate Math Lab*

Peter Sarnak†, Steven Miller‡, Alex Barnett§

September 11th, 2002

Courant Institute of Mathematics
New York University
New York, NY

Abstract

We review the Legendre Symbol. We discuss Gary Miller's primality test, and show that if the General Riemann Hypothesis (for Dirichlet Characters) is true, then Miller's test correctly determines if a number n is prime or composite, and runs in time $O(\log^4 n)$. Lecture by Peter Sarnak; notes by Steven Miller.

1 Review of the Legendre Symbol

Recall Fermat's Little Theorem: $a^{p-1} \equiv 1 \bmod p$ if p is prime.

Given n, check $a^{n-1} \equiv 1 \bmod n$ for many a's relatively prime to n. **Exercise:** If ever this is not satisfied, then n *must* be composite.

There are composite numbers (called Carmichael numbers) which satisfy $a^{n-1} \equiv 1 \bmod n$ for all a, yet are not prime. The first Carmichael number is $561 = 3 \cdot 11 \cdot 17$; the third is $1729 = 7 \cdot 13 \cdot 19$. **Exercise:** Prove all Carmichael numbers *must* be square-free.

Aside: 1729 has an interesting history (Ramanujan, Hardy and taxicabs). Hardy visited Ramanujan in the hospital, Hardy remarked that his taxicab's

*Homepage: http://www.math.nyu.edu/∼millerj/
†E-mail: sarnak@math.princeton.edu
‡E-mail: millerj@cims.nyu.edu or sjmiller@math.princeton.edu
§E-mail: barnett@nmr.mgh.harvard.edu

number was particularly uninteresting; Ramanujan remarks it (1729) is the smallest number which can be written in two different ways as the sum of two cubes. $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

Recall the **Legendre symbol** $\left(\frac{a}{p}\right)$ is 0 if $p|a$, 1 if there is an $x \neq 0$ with $x^2 \equiv a \bmod p$, and -1 if there is no solution to $x^2 \equiv a \bmod p$. **Euler's condition** is $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.

Really, the Legendre symbol is a function on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We can extend the Legendre symbol to all integers. We only need to know $a \bmod p$, and we define $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$.

Initially the Legendre symbol is define only when the bottom is prime. We now extend the definition to all n as follows: let $n = p_1 \cdot p_2 \cdots p_t$ be the product of t distinct primes. Then $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$. Note this is *not* the same as saying that if a is a square (a quadratic residue) mod n, then a is a square mod p_i for each prime divisor.

The main result (which allows us to calculate the Legendre symbol quickly and efficiently) is the celebrated

Theorem 1.1 (Quadratic Reciprocity) *For m, n odd and relatively prime,* $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

2 Gary Miller's Primality Test, 1976

Miller Test: *Given n as input (n must be odd), test whether for $2 \leq a \leq 70\log^2 n$, $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ (where, of course, a and n are relatively prime). If this test fails for some a in this range, output* composite*; if it passes the test for all such a, output* Prime*.*

Note that we can very quickly determine if two number are relatively prime (use the Euclidean Algorithm, which takes $O(\log n)$ steps).

Theorem 2.1 (Miller Test Results) *The Miller Test runs in $O(\log^4 n)$ steps. If the output is* composite*, then the number n* is *composite (ie, the algorithm's result is correct). If we assume GRH (the* General Riemann Hypothesis*, the most important unsolved problem in mathematics), then the output* prime *is also correct.*

Running time: we can compute $\left(\frac{a}{n}\right)$ in $O(\log n)$ steps. By Quadratic Reciprocity, to compute $\left(\frac{a}{n}\right)$ (may assume $-\frac{n}{2} \leq a \leq \frac{n}{2}$), it is enough to compute $\left(\frac{n}{a}\right)$ (with a factor of -1).

Why? We only need to know a mod n, so we may reduce a until $-\frac{n}{2} \leq a \leq \frac{n}{2}$. Note the top (in absolute value) is at most half the size of the bottom (n). We then use quadratic reciprocity to evaluate $\left(\frac{a}{n}\right)$. Up to a factor of -1, $\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$. Thus, we may reduce n mod a, so that n mod a lies between $-\frac{a}{2}$ and $\frac{a}{2}$. Again, the top is half the bottom, and the bottom is at most one-quarter of what we started with (n).

We continue this process; we need to do such flippings at most $\log n$ times. Why? Each time the size of the denominator is at most half what it was before. If $2^r = n$, then $r = \log_2 n < \log n$. Thus, after at most $\log n$ passes, the denominator would be about 1. So, a stage or two before would give a denominator around 2 or 4. The point is, in $\log n$ steps, we can reduce to evaluating the Legendre symbol of something where the bottom is of bounded size. Thus, we can evaluate $\left(\frac{a}{n}\right)$ in $O(\log n)$ steps. (Have a lookup table for $n < 10$, et cetera).

We need to evaluate $\left(\frac{a}{n}\right)$ for $C \log^2 n$ choices of a, and for each choice we need to evaluate $a^{\frac{n-1}{2}}$ mod n (so we can compare it to $\left(\frac{a}{n}\right)$), which takes $O(\log n)$ steps. Thus, the number of steps is $O(\log^4 n)$.

The Riemann Hypothesis plays a very important catalystic role. It leads us to statements we feel should be true, statements which can often be proved without the full force of Riemann.

Suppose we pass the test for all a with $2 \leq a \leq 70 \log^2 n$ and a relatively prime to n. Gary Miller proved that, if GRH is true, then knowing that n passes the test for all a in this little segment allows us to conclude that n will pass the test *for all* a. Clearly, we know if n passes the test for all a up to $n-1$, then we know n will pass the test for all a relatively prime to n. The power of GRH is that we need only check $\log^2 n$ values of a.

2.1 Aside: Finite Abelian Groups

Let A be a finite Abelian Group, then A is (ie, is isomorphic to) a product of cyclic groups.

Look at $(\mathbb{Z}/n\mathbb{Z}, +)$, the group of integers mod n under clock addition. This is a cyclic group.

The general statement is:

Theorem 2.2 (Structure Theorem for Finite Abelian Groups) *Let A be a finite Abelian Group. Then there are integers n_1 through n_t such that*

$A \approxeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, ie, A is isomorphic to the Cartesian product of groups of the form $\mathbb{Z}/m\mathbb{Z}$.

Note $\approxeq$ means is isomorphic to; we say two groups are **isomorphic** if there is a group homomorphism between them which is one-to-one and onto. A **group homomorphism** ϕ is a map which preserves the group structure. Consider two groups G_1 and G_2 and a map $\phi : G_1 \to G_2$. If ϕ is a group homomorphism, then for $x, y \in G_1$, $\phi(x + y) = \phi(x) \bigoplus \phi(y)$, where $+$ is addition in the first group and $\bigoplus$ is addition in the second group.

We now define the **Cartesian Product** of two groups. $X \times Y$ is the set of pairs (x, y) where $x \in X$ and $y \in Y$. If we are writing the group action of X and Y additively (say by $\bigoplus_X$ for addition in X and $\bigoplus_Y$ for addition in Y), then $(x_1, y_1) \bigoplus_{X+Y} (x_2, y_2) = (x_1 \bigoplus_X x_2, y_1 \bigoplus_Y y_2)$.

Let us consider a group written in additive notation. Recall the **order of an element** is the number of times you must add the element to itself to get the identity. We define the **exponent** of a group as the least common multiple of the orders of the elements of the group.

Consider $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, the product of two groups. In $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, we have the pairs $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$. $(0, 0)$ is the identity under addition; all other elements (check) have order 2. Thus, the exponent of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is 2.

Now consider $\mathbb{Z}/4Z = \{0, 1, 2, 3\}$. 0 is the identity, and under addition 1 and 3 have order 4, and 2 has order 2. Thus, the exponent of this group is 4. **Exercise:** using the exponent, observe that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4Z$ cannot be isomorphic.

Fact: if p is prime, then $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field. The non-zero elements have multiplicative inverses. $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ (the non-zero elements under multiplication) is a cyclic abelian group with $p-1$ elements! IE, there is an element g whose powers generate the group. **Exercise:** Prove that if n is composite, then $\mathbb{Z}/n\mathbb{Z}$ is not a field. Hint: show some non-zero element has no multiplicative inverse.

Sketch of Proof of Fact: Suppose $\mathbb{F}_p^*$ is not cyclic. Let d be the exponent (the least common multiple of the orders of the elements) of $\mathbb{F}_p^*$. Then $d < p - 1$. As the order of every element divides $p - 1$ (Lagrange's Theorem), we have $d|p - 1$.

For each $x \in Fpf$, $x^d = 1$ (in the field $\mathbb{F}_p^*$). This is because d is the least common multiple of the orders of the elements of the group. Thus, if $\mathrm{ord}(x)$

is the order of x, $x^{\text{ord}(x)} = 1$. As $\text{ord}(x)|d$, we have $\text{ord}(x) = kd$ for some $k \in \mathbb{Z}$. Thus, $x^d = x^{k\text{ord}(x)} = (x^{\text{ord}(x)})^k = 1^k = 1$.

Now use the fact that $\mathbb{F}_p^*$ is a field. Consider $x^d - 1 = 0$ over $\mathbb{F}_p$ (clearly 0 is not a root). **Over** $\mathbb{F}_p$ means look for solutions to this equation with $x \in \mathbb{F}_p$). A polynomial of degree d has at most d roots (another theorem of Lagrange). But every $x \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ is a root, because d (the exponent of the group) is the least common multiple of the orders of the elements. This is a contradiction: we have $p-1$ roots (every $x \in \mathbb{F}_p^*$ solves $x^d - 1 \equiv 0 \mod p$), but by Lagrange there are at most d roots. As $d < p-1$, contradiction.

Steve Miller will discuss this needed theorem of Lagrange. See also the handout from Davenport's *The Higher Arithmetic*.

2.2 Lehmer's Proposition

Proposition 2.3 (Lehmer) *If* $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$ *mod* n *for all* a *up to* $C \log^2 n$, *then* n *is prime.*

We assume $n = p_1 \cdots p_t$, $t > 1$, and all primes are distinct and odd. (When there are repeated primes, the proof is easier, and is left as an exercise to the reader). Then $a^{n-1} \equiv 1 \mod n$ for $(a, n) = 1$ (ie, a and n relatively prime), implies that $a^{n-1} \equiv 1 \mod p_j$ (p_j one of the prime factors of n).

Thus, $n - 1 \equiv 0 \mod p_j - 1$. If there were a remainder (ie, if $n-1$ wasn't equivalent to 0 mod $p_j - 1$ but was equivalent to $r_j \not\equiv 0 \mod p_j - 1$), if we raised a to this power (r_j), we wouldn't get 1 for all a. Just take a a generator of $\mathbb{F}_{p_j}^*$, ie, an element of maximal order $p_j - 1$. Then $a^{n-1} \equiv a^{r_j} \not\equiv 1 \mod p_j$. Note that $a^{p_j - 1} \equiv 1 \mod p_j$, so $a^{n-1} \equiv a^{r_j} \mod p_j$.

We say p_j (a factor of n) is **of type** 1 if $\frac{n-1}{2} \equiv 0 \mod p_j - 1$; we say p_j is **of type** 2 if $\frac{n-1}{2} \equiv \frac{p_j - 1}{2} \mod p_j - 1$.

If at least one of the p_j's (without loss of generality, say p_1) is of type 1, take a a quadratic non-residue mod p_1 and a quadratic residue for p_2, $p_3, \dots, p_t$. One can find such an a by the **Chinese Remainder Theorem** as the primes are distinct. For a statement of the Chinese Remainder Theorem, see the Appendix at the end of the notes.

We have $\left(\frac{a}{p_1}\right) = -1$ and $\left(\frac{a}{p_j}\right) = 1$ for $j > 1$. As we are assuming n is composite, there are at least two primes.

As $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_t}\right)$, we obtain $\left(\frac{a}{n}\right) = -1 \cdot 1 \cdots 1$.

As we are assuming p_1 is of type 1, we have $\frac{n-1}{2} \equiv 0 \bmod p_1 - 1$. Mod $p_1 - 1$, each non-zero element in $(\mathbb{F}/p_1\mathbb{F})^*$ has order dividing $p_1 - 1$. Thus, $a^{\frac{n-1}{2}} \equiv 1 \bmod p_1$.

We are assuming that the Miller Test is satisfied for all a. Thus, $\left(\frac{a}{n}\right) = a^{\frac{n-1}{2}} \bmod n$. Mod p_1, we have shown the left hand side is -1 and the right hand side is 1, contradiction!

We are left with the case where all the primes are of type 2. We leave this as an exercise for the reader.

3 GRH Implies Just Need To Check Up To $O(\log^2 n)$ in Miller

Why does GRH imply that $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ for all a up to $70\log^2 n$ (and relatively prime to n) implies that $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ for all a relatively prime to n?

3.1 Fourier Analysis

Representation Theory (especially characters of Abelian Groups) is the most important things in Mathematics. Let A be a finite Abelian Group. To each such group, we associate a dual group, denoted $\hat{A}$, where $\hat{A}$ is the set of all homomorphisms from A into $\mathbb{C}^*$, $\mathbb{C}^*$ are the complex numbers invertible under multiplication.

Recall ψ is a *group homomorphism* if $\psi(a+b) = \psi(a)\psi(b)$. Note here $\psi : G_1 \to G_2$, and G_1 has been written additively and G_2 has been written multiplicatively. We call such a ψ a *character*.

3.2 Examples

Let $A = \mathbb{Z}/n\mathbb{Z}$, and $\nu \in \mathbb{Z}/n\mathbb{Z}$. Let $e(z) = e^{2\pi i z}$ for $z \in \mathbb{C}$. Define $\psi_\nu(x) = e(\frac{\nu x}{n})$. **Exercise:** Show by direct calculation that $\psi_\nu(a+b) = \psi_\nu(a)\psi_\nu(b)$. In fact, for each $\nu \in \mathbb{Z}/n\mathbb{Z}$ we get a character, and the characters are distinct (exercise). We only need to know how ψ_ν acts on 1, as $\psi_\nu(k) = \psi_\nu(1 + \cdots + 1) = \left(\psi_\nu(1)\right)^k$. $\hat{A}$ is canonically isomorphic to A. What this means is, to each $\nu \in A$ there corresponds a character ψ_ν in $\hat{A}$, and to each character $\psi \in \hat{A}$ there corresponds a number $\nu_\psi \in A = \mathbb{Z}/n\mathbb{Z}$.

We can multiply two characters: $(\psi_1\psi_2)(x) = \psi_1(x)\psi_2(x)$. It is easy to see that this is a character. The trivial character (which sends everything to 1) is the identity of the group $\hat{A}$.

Consider two groups A and B. We can use the characters of A and B to get the characters of the cartesian product $A \times B$. If we want the characters of $A \times B$, take a character ψ_a of A and ϕ_b of B and form the character $\psi_a\phi_b$, defined by $(\psi_a\phi_b)(x,y) = \psi_a(x)\phi_b(y)$.

3.3 Characters of $\mathbb{F}_p^*$: Dirichlet Characters

We denote characters of $\mathbb{F}_p^*$ by χ. Dirichlet proved the best theorem of mathematics, introducing a lot of new math to solve the following:

Theorem 3.1 (Primes in Arithmetic Progressions, 1836, 1839) *Let a and n be relatively prime. There are infinitely many primes which give a when divided by n; moreover, to first order all residue classes a mod n (a, n relatively prime) have the same number of primes!*

In other words, there are infinitely many x such that $xn + a$ is prime if a and n are relatively prime.

Hard Question: without using Dirichlet's Theorem, can you prove that there must be *one* prime congruent to a mod n if a and n are relatively prime?

Clearly, if a and n are not relatively prime, there cannot be infinitely many primes congruent to a mod n. Dirichlet shows this is also a sufficient condition.

Dirichlet introduced characters *without* introducing the concept of a group! They didn't have group notation until later.

Look at $(\mathbb{Z}/n\mathbb{Z})^* = \{x : (x,n) = 1, 0 < x \leq n-1\}$. This is a finite Abelian group. $\#(\mathbb{Z}/n\mathbb{Z})^* = \phi(n)$, where $\phi(n)$ is the Euler totient function, and $\phi(n)$ is the number of integers (between 0 and n) which are relatively prime to n.

Dirichlet used q instead of n, so we change notation and look at $(\mathbb{Z}/q\mathbb{Z})^*$.

A **Dirichlet Character** is a character χ of $(\mathbb{Z}/q\mathbb{Z})^*$; ie, $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ and $\chi(ab) = \chi(a)\chi(b)$. Thus, χ lies in the dual group of $(\mathbb{Z}/q\mathbb{Z})^*$. Recall that $\mathbb{C}^*$ is the set of complex numbers with multiplicative inverses, ie, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

The **principal or trivial character** takes every $x \in (\mathbb{Z}/q\mathbb{Z})^*$ to 1; we denote the trivial character by χ_0.

If χ is a Dirichlet Character of $(\mathbb{Z}/q\mathbb{Z})^*$, we say χ has **modulus** (also called **conductor**) q. We extend χ to be defined on all integers (all of $\mathbb{Z}$) by $\chi(m) = 0$ if m and q are not relatively prime, and $\chi(m) = \chi(m \bmod q)$ otherwise. Clearly χ is periodic, as $\chi(x + \lambda q) = \chi(x)$ for any $\lambda \in \mathbb{Z}$. Thus, we have the map $\chi : \mathbb{Z} \to \mathbb{C}^*$.

If q is prime, we have previously seen the character $\chi(a) = \left(\frac{a}{q}\right)$. This is an extremely important character.

Another example: Let $q = 4$. We define $\chi(n)$ to be 0 if n is even, 1 if $n \equiv 1 \bmod 4$, and -1 if $n \equiv -1 \bmod 4$. **Exercise:** Show this is a character.

3.4 General Riemann Hypothesis (GRH)

Below, p will always denote a prime. χ will be a Dirichlet character modulo q (q need not be prime).

Conjecture: GRH: *For any $q \geq 1$, $x \geq 3$, if $\chi \neq \chi_0$ (ie, if χ is not the principal character) then*

$$\Big|\sum_{p \leq x} \Big(1 - \frac{p}{x}\Big) \cdot \log p \cdot \chi(p)\Big| \leq C \log q \cdot \sqrt{x}. \tag{1}$$

If $\chi = \chi_0$, then

$$\sum_{p \leq x} \Big(1 - \frac{p}{x}\Big) \log p \leq \frac{x}{2} + O(\sqrt{x}). \tag{2}$$

C is a universal constant, independent of q.

We are summing primes up to x. The $1 - \frac{p}{x}$ factors are just weight factors. If $q = 4$ and χ is the character above, $\chi(p)$ gives a positive sign for primes congruent to 1 mod 4 and a minus sign for primes congruent to -1 mod 4.

Analysis means cancellation; you want to see cancellation in a sum. The numbers in these sums are flipping (plus one, minus one); we have about $\frac{x}{\log x}$ primes less than x (this is the Prime Number Theorem, first proved in 1896).

Random Drunk: each moment he flips a coin. If it is heads he staggers one unit left, tails he staggers one unit right. After n steps, where do you think he'll be? Turns out he'll be about $\sqrt{n}$ units from the origin (with high probability). Steve Miller will prove this in a later lecture or handout.

Motto: random numbers (of size around 1) cancel like the square-root of the number of terms.

What GRH is telling us is that the remainder term behaves like random noise.

3.5 Proof of the Miller Test

Theorem 3.2 *If GRH is true, then if $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$ for all $a \leq C \log^2 n$ for some fixed constant C, then it is true for all a (relatively prime to n, of course).*

Remarkable observation: $S = \{a \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Why? Exercise (Closure: show if a, b in this set, so is ab. Identity: show 1 is in this set. Inverses: show if $a \in S$, $a^{-1} \bmod n$ is in S. Note associativity is inherited from $(\mathbb{Z}/n\mathbb{Z})^*$).

By assumption, S contains (at least) the first $C \log^2 n$ elements. We claim this implies S contains all a relatively prime to n.

Suppose S is not all of $(\mathbb{Z}/n\mathbb{Z})^*$. We talked about cosets (of Abelian Groups) last time. (For more information about cosets and quotient groups, see the following lecture by Steven Miller, notes by Alex Barnett). As everything is abelian, we can form a quotient group by dividing our group $(\mathbb{Z}/n\mathbb{Z})^*$ by the abelian subgroup S.

Thus, $A = \frac{(\mathbb{Z}/n\mathbb{Z})^*}{S}$ is a group (a quotient group) and A is a non-trivial group (ie, there is more than one element in this group). Why must A have more than one element? A is the group of representative cosets of $(\mathbb{Z}/n\mathbb{Z})^*$ by the abelian subgroup S. As S is not all of $(\mathbb{Z}/n\mathbb{Z})^*$, there must be at least two cosets. Hence A is not just the identity coset (which is $1 \cdot S$ or just S).

But this quotient (A) is a finite abelian group. We know for a finite abelian group that its dual is isomorphic to itself. This means to each element in A we have a character in $\hat{A}$, and vice-versa. Further, the identity of A is mapped to the trivial character of $\hat{A}$.

Thus, there is a non-trivial $\chi : A \to \mathbb{C}^*$. Now $(\mathbb{Z}/n\mathbb{Z})^* \to \frac{(\mathbb{Z}/n\mathbb{Z})^*}{S} \to \mathbb{C}^*$, and thus we have a non-trivial Dirichlet character of $(\mathbb{Z}/n\mathbb{Z})^*$ which is trivial on S (ie, $\chi(s) = 1$ for all $s \in S$).

By construction, χ is a Dirichlet character of $(\mathbb{Z}/n\mathbb{Z})^*$, $\chi \neq \chi_0$, and $\chi|_S = 1$ (the last means that χ, **restricted to** $s \in S$ is the identity map). We know S is all elements up to at least $C \log^2 n$. So, $\chi(a) = 1$ for all $a \leq C \log^2 n$ (from the givens).

So, look at

$$\mathrm{Sum}(p,q,x) = \sum_{p\le x}\left(1-\frac{p}{x}\right)\log p\cdot\chi(p). \tag{3}$$

By GRH, $\mathrm{Sum}(p,q,x)$ is less than a constant multiple of $\log q\cdot\sqrt{x}$. Calling the constant C_2, we have $\mathrm{Sum}(p,q,x) \le C_2\log q\cdot\sqrt{x}$.

If $x \le C\log^2 n$, then there is a contradiction. Why? In Equation 3, $\mathrm{Sum}(p,q,x)$ is going to be $\sum_{p\le x}\left(1-\frac{p}{x}\right)\log p$, because all the $\chi(p)=1$ in this range. The **Prime Number Theorem** states that the number of primes less than x is $\frac{x}{\log x}$ plus an error term which is smaller than $\frac{x}{\log x}$ (ie, in the limit, the size of the error term divided by the number of primes less than x tends to 0 as x goes to infinity).

Thus,$\mathrm{Sum}(p,q,x)$ is going to look like a multiple of x. Why a multiple of x and not a multiple of $\frac{x}{\log x}$? Remember we have the factor $\log p$ in the sum; this follows from **Partial Summation**. Partial Summation is a discrete version of Integration by Parts; see the Appendices at the end for a further statement.

By GRH, $\mathrm{Sum}(p,q,x)$ is bounded by $C_2\log q\cdot\sqrt{x}$. Therefore, $x \le C_2\log q\cdot\sqrt{x}$. This implies $\sqrt{x} \le C_2\log q$, or $x \le C_2^2\log^2 q$.

Remember, we've changed notation from n to q. We are assuming that $\left(\frac{a}{q}\right) \equiv a^{\frac{q-1}{2}}$ mod q for all $a \le C\log^2 q$ for some fixed constant C. Take C greater than C_2^2. Then we have a contradiction! If GRH is true, $\mathrm{Sum}(p,q,x) \le C_2\log q\cdot\sqrt{x}$ only for $x \le C_2^2\log^2 q$. But we are assuming that q passes the Miller Test for all a up to $C\log^2 q$. Thus, we can take x larger than $C_2^2\log^2 q$.

3.6 Review of Proof

Intuition: For random sequences, expect square-root cancellation in sums.

If we have a non-trivial character, if we look at these weighted sums of $\chi(p)$, there is no extra structure; we expect cancellation like $\sqrt{x}$. There has to be *some* q-dependence, but GRH says it is like a universal constant times $\log q$.

In the Miller Test, we test something $C\log^2 n$ times. If the condition is always true for these $C\log^2 n$ elements, we have a subgroup S of $(\mathbb{Z}/n\mathbb{Z})^*$. If S isn't all of $(\mathbb{Z}/n\mathbb{Z})^*$, we can find a character, and we have sums with this character (any sum with characters is called **Harmonic Analysis**). Further, this is a non-trivial character which is the identity on the original group. The GRH cannot accomodate a character of this type.

Why does the GRH lead to a contradiction? Basically, GRH says a certain weighted sum of $\chi(p)$ over the primes less than x (where χ is a Dirichlet character with modulus q) cannot be too large. Specifically, it is at most $C_2 \log q \cdot \sqrt{x}$.

This implies that there is a lot of noise in the $\chi(p)$; basically, we need to have a good mixing of primes which give $\chi(p) = +1$ with primes giving $\chi(p) = -1$.

However, if n satisfies the Miller Test for a up to $C \log^2 q$ (with $C > C_2^2$), then we can find a modulus q and a Dirichlet character χ where we have a very long string of primes giving $\chi(p) = +1$. This forces the weighted sum of $\chi(p)$ over primes less than x (taking $x = C \log^2 q$) to be larger than $C_2 \log q \sqrt{x}$, a contradiction.

4 Appendices

4.1 Aside: For p Odd, Half the Non-Zero Numbers are Quadratic Residue

Note, for an odd prime p_j, half of the non-zero numbers are quadratic residues, and half are quadratic non-residues. The **Legendre symbol** takes each element $a \in \mathbb{F}_p^*$ to an element in the group $\{-1, 1\}$. This is a homomorphism; not every element has a square. The image is $\{-1, 1\}$; the kernel is all the elements of $\mathbb{F}_p^*$ which are sent to 1. Thus, half the numbers are residues, half are non-residues.

$a \to \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$. Thus, we have a homomorphism (given by the Legendre symbol) from $\mathbb{F}_p^* \to \{-1, 1\}$. We claim the map is onto. The kernel is all elements in $\mathbb{F}_p^*$ which are mapped by the Legendre symbol to 1, ie, the quadratic residues. (One needs to show the Legendre symbol is a group homomorphism: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{y}{p}\right)$).

Standard Group Theory Arguments: $\frac{\#\mathbb{F}_p^*}{\text{kernel}} \approxeq \{-1, 1\}$. Thus, half the numbers in $\mathbb{F}_p^*$ are quadratic residues.

4.2 Chinese Remainder Theorem

Theorem 4.1 (Chinese Remainder Theorem) *Let $m = m_1 m_2$, m_1 and m_2 relatively prime. Then $\mathbb{Z}/m\mathbb{Z} \approxeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$.*

This allows us to, given a_1 mod m_1 and a_2 mod m_2, find an a mod m such that $a \equiv a_1$ mod m_1 and $a \equiv a_2$ mod m_2. For example, try and solve $x \equiv 3$ mod 5 and $x \equiv 4$ mod 7.

See any book on Algebra.

4.3 Partial Summation

Lemma 4.2 (Partial Summation: Discrete Version)

$$\sum_{M}^{N} a_n b_n = A_N b_N - A_{M-1} b_M + \sum_{M}^{N-1} A_n (b_n - b_{n+1}) \tag{4}$$

Lemma 4.3 (Abel's Summation Formula - Integral Version) *Let $h(x)$ be a continuously differentiable function. Let $A(x) = \sum_{n \leq x} a_n$. Then*

$$\sum_{n \leq x} a_n h(n) = A(x)h(x) - \int_1^x A(u)h'(u)du \tag{5}$$

See, for example, Walter Rudin, *Principles of Mathematical Analysis* (also known as *The Blue Book*), page 70.