Dirichlet's Theorem on Primes in an Arithmetic Progression

Daniel Weissman

May 24, 2004

1 Introduction and References

Our goal is to prove the following theorem:
Dirichlet's Theorem: For any coprime $a, b \in \mathbf{Z}$, there are infinitely many primes p such that $p \equiv a \pmod{b}$.

Although the statement of the theorem involves only integers, the simplest proof requires the use of complex numbers and Dirichlet L-series. Most of this paper will therefore be devoted to proving some basic properties of characters and L-series, after which the desired theorem will follow fairly easily.

The main sources for the following proof are Daniel Marcus' *Number Fields* and Chapter 7 from Chan Heng Huat's online course notes from MA 4263: Analytic Number Theory at the National University of Singapore (available at http://www.math.nus.edu.sg/~chanhh/MA4263/MA4263.html), especially the latter. Marcus proves a more general result, while Chan's proof is a little easier to follow. In addition, our proof that $\sum_p \frac{1}{p^s}$ diverges as $s \to 1^+$ is based on arguments in Joseph Bak and Donald Newman's *Complex Analysis*, and the discussion of Chebotarev's Density Theorem follows H. P. F. Swinnerton-Dyer's *A Brief Guide to Algebraic Number Theory*. The latter book also contains a proof of Dirichlet's Theorem, but Swinnerton-Dyer is not as easy to understand as Marcus and Chan.

For those who would like to read a little more about the subject, Atle Selberg's "An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression" (*The Annals of Mathematics*, Vol. 50, No. 2 (Apr., 1949), 297-304) proves the theorem without using complex numbers. However, the proof is long and not particularly enlightening. (I also think that the techniques probably do not generalize as well as the ones used in our proof.) The more general Chebotarev Density Theorem is proved in Swinnerton-Dyer (although I do not know how understandable the proof is), and Marcus provides the outlines of a proof and leaves the rest as an exercise.

2 Characters

We will define characters for finite abelian groups. They can be defined for general groups, but our proof will only use the characters of the group $(\mathbf{Z}/b\mathbf{Z})^*$, so this definition will be sufficient.

Definition: A character χ of a finite abelian group G is a homomorphism $\chi : G \to \mathbf{C}^*$ taking G to the unit circle. Note that the characters of a finite abelian group are exactly the one-dimensional group representations. The characters of more general groups do not have this property.

The finite multipicative subgroups of $\mathbf{C}^*$ are just the n^{th} roots of unity, so each character maps G to the n^{th} roots of unity for some $n \geq 1$. Note that since χ is a group homomorphism, its kernel is a subgroup $H \subset G$, and it maps each H-coset of G to a distinct root. It therefore maps an equal number of elements of G to each root of unity.

We define multiplication of characters by

$$\chi\chi' : g \mapsto \chi(g)\chi'(g). \tag{1}$$

Note that with this definition of multiplication, the characters form a group, which is usually called $\hat{G}$. We will denote the identity element (which maps G to 1) by χ_0. Note also that, because the characters map to the unit circle, $\chi^{-1}(g) = 1/\chi(g) = \overline{\chi(g)}$, the complex conjugate of $\chi(g)$. We will therefore write the inverse of χ as $\bar{\chi}$. One important property of the character group is that it is isomorphic to G.

Lemma: $\hat{G} \cong G$.

Proof: Since G is a finite abelian group, we can write

$$G \cong \mathbf{Z}/(d_1) \oplus \mathbf{Z}/(d_2) \oplus \ldots \oplus \mathbf{Z}/(d_k) \tag{2}$$

with $d_1|d_2|\ldots|d_k$. We can write each element of G as $(e_1, \ldots, e_k)$, $e_i \in \mathbf{Z}/(d_i)$. G will be generated by $a_1 = (1, 0, \ldots, 0)$, $a_2 = (0, 1, 0, \ldots, 0)$, $\ldots$,

$a_k = (0, 0, \ldots, 0, 1)$, with each a_i having order d_i. Each character χ must map each a_i to one of the d_i^{th} roots of unity. If we let $\zeta_{d_i} = e^{2\pi i/d_i}$, then $\chi(a_i) = \zeta_{d_i}^{e_i}$, $e_i \in \mathbf{Z}/(d_i)$. Each χ will be determined by its values on the a_i, so we can specify χ by the k-tuplet $(e_1, \ldots, e_k)$. Any possible sequence of values for the e_i defines a valid character, so there is an obvious bijection between G and $\hat{G}$. This bijection clearly respects the group law.

Corollary: The characters satisfy two important identities:

$$(i) \sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0; \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

$$(ii) \sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1; \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Proof: (i) This follows immediately from the fact that χ sends an equal number of elements of G to each d^{th} root of unity, and that the sum of the d^{th} roots of unity is 0 for $d > 1$.

(ii) If $g = 1$, then $\chi(g) = 1$ for all χ, so $\sum_{\chi \in \hat{G}} \chi(g) = |\hat{G}| = |G|$. ($|\hat{G}| = |G|$ since $\hat{G} \cong G$.) If $g \neq 1$, then $\exists \chi_1 \in \hat{G}$ such that $\chi_1(g) \neq 1$. (Otherwise, $\hat{G}$, and thus also G, would be the trivial group, and we would not be able to find an element $g \neq 1$.) We can write

$$\begin{aligned} \sum_{\chi \in \hat{G}} \chi(g) &= \sum_{\chi \in \hat{G}} \chi_1 \chi(g) \\ &= \chi_1(g) \sum_{\chi \in \hat{G}} \chi(g), \end{aligned}$$

so we must have $\sum_{\chi \in \hat{G}} \chi(g) = 0$.

3 Dirichlet L-series

If $G = (\mathbf{Z}/b\mathbf{Z})^*$, then we can extend the characters of G to all $n \in \mathbf{Z}$ by letting

$$\chi(n) = \begin{cases} \chi(\bar{n}) & \text{if } \bar{n} \in (\mathbf{Z}/b\mathbf{Z})^*; \\ 0 & \text{otherwise,} \end{cases}$$

where $\bar{n}$ is the residue class of $n \pmod b$. Note that these *Dirichlet characters* form a group canonically isomorphic to $\hat{G}$, so all the results proved in the previous section carry over in the obvious ways. For the rest of the paper, we will use "character," "χ," and "$\hat{G}$" to refer to the Dirichlet characters of $G = (\mathbf{Z}/b\mathbf{Z})^*$. Note that with this definition we have $|G| = \phi(b)$, where ϕ is Euler's function.

The Dirichlet L-series is then defined for $s \in \mathbf{C}$ and $\chi \in \hat{G}$ by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{5}$$

Since $|\chi(n)| = 1$, the series will converge absolutely iff $\Re(s) > 1$. For our proof, we will need to show that it converges conditionally on $\Re(s) > 0$ (except for $s = 1$, $\chi = \chi_0$), and that it is nonzero at $s = 1$. To do this, we will first show that we can also write $L(s,\chi)$ as an infinite product. Note that since

$$L(s,\chi) = 1 + \frac{\chi(2)}{2^s} + \frac{\chi(3)}{3^s} + \dots,$$

we have, for example,

$$\frac{\chi(2)}{2^s} L(s,\chi) = \frac{\chi(2)}{2^s} + \frac{\chi(4)}{4^s} + \frac{\chi(6)}{6^s} + \dots$$

so that

$$\left(1 - \frac{\chi(2)}{2^s}\right) L(s,\chi) = 1 + \frac{\chi(3)}{3^s} + \frac{\chi(5)}{5^s} + \dots,$$

and in general

$$\left(1 - \frac{\chi(p)}{p^s}\right) L(s,\chi) = \sum_{n \notin (p)} \frac{\chi(n)}{n^s}.$$

Repeating the process for all primes gives:

$$\prod_p \left(1 - \frac{\chi(p)}{p^s}\right) L(s,\chi) = 1,$$

so we have

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{6}$$

Lemma: For $\chi \neq \chi_0$, $L(s,\chi)$ converges in the region $\Re(s) > 0$. $L(s,\chi_0)$ converges for $\Re(s) > 0$ except at $s = 1$, where it has a simple pole.

Proof: By (3), we know that for $\chi \neq \chi_0$,

$$\sum_{n=N+1}^{N+b} \chi(n) = \sum_{\bar{n} \in (\mathbf{Z}/b\mathbf{Z})^*} \chi(\bar{n}) = 0,$$

so the partial sums of the sequence $\chi(n)$ for $n = 1, 2, 3, \ldots$ are bounded by the constant $\max_{1 \leq N \leq b} \sum_{n=1}^{N} \chi(n)$. Since $\Re(s) > 0$, the sequence $\frac{1}{n^s}$ is converging monotonically to 0, so $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges by Dirichlet's Test.

For $\chi = \chi_0$, we have

$$\begin{aligned} L(s,\chi_0) &= \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} \\ &= \prod_{p \nmid b} \left(1 - \frac{1}{p^s}\right)^{-1} \\ &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p|b} \left(1 - \frac{1}{p^s}\right) \\ &= \zeta(s) \prod_{p|b} \left(1 - \frac{1}{p^s}\right), \end{aligned}$$

where $\zeta(s)$ is the Zeta Function, which has an analytic extension to $\Re(s) > 0$ except at $s = 1$, where it has a simple pole with residue 1.

Corollary: $L(1,\chi) \neq 0$.

Proof: We have already seen that $L(s,\chi_0)$ has a simple pole at $s = 1$. Let $P(s) = \prod_{\chi \in \hat{G}} L(s,\chi)$. P is the product of analytic functions on $\Re(s) > 0$, so it is analytic, except possibly for a simple pole at $s = 1$. Since P is meromorphic, it is continuous on $\Re(s) > 0$ (when viewed as a map $\mathbf{C} \to \hat{\mathbf{C}}$). Let us assume that none of the functions $L(s,\chi), \chi \in \hat{G}$, are uniformly zero on $Re(s) > 0$. Then, because they are meromorphic, $\forall \delta > 0, \exists x \in \mathbf{R}_{>1}$ with $|x - 1| < \delta$ such that $\forall \chi \in \hat{G}, L(x,\chi) \neq 0$ (because otherwise we would have an infinite sequence of zeroes with an accumulation point) For such x, $P(x) \neq 0$, and we can take the log:

$$\ln(P(x)) = \sum_{\chi \in \hat{G}} \ln\left(L(x,\chi)\right)$$

$$
\begin{aligned}
&= \sum_{\chi \in \hat{G}} \ln \left(\prod_p \left(1 - \frac{\chi(p)}{p^x}\right)^{-1} \right) \\
&= -\sum_{\chi \in \hat{G}} \sum_p \ln \left(1 - \frac{\chi(p)}{p^x}\right) \\
&= \sum_{\chi \in \hat{G}} \sum_p \sum_{n=1}^{\infty} \frac{\chi^n(p)}{np^{xn}} \\
&= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{xn}} \sum_{\chi \in \hat{G}} \chi(p^n),
\end{aligned}
$$

where we can switch the order of the sums because they are absolutely convergent for our choice of x. Note that we have used the fact that the analytic continuation of $\ln(1-y)$ to the complex numbers is $\ln(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$ for $|z| < 1$. By (3), the sum is non-negative, so $\ln(P(x)) \geq 0$, and thus $P(x) \geq 1$ for x on the positive real line arbitrarily close to 1. Now suppose that for some $\chi \in \hat{G}$ we have $L(1, \chi) = 0$. We know that $L(s, \chi_0)$ has a simple pole at 1, so $\chi \neq \chi_0$, and therefore $\bar{\chi} = \chi^{-1} \neq \chi$. However, we still have

$$
\begin{aligned}
L(1, \bar{\chi}) &= \sum_{n=1}^{\infty} \frac{\bar{\chi}(n)}{n} \\
&= \overline{\sum_{n=1}^{\infty} \frac{\chi(n)}{n}} \\
&= \overline{L(1, \chi)} \\
&= 0,
\end{aligned}
$$

so there are at least two $\chi \in \hat{G}$ for which $L(1, \chi) = 0$. χ_0 is the only character for which $L(1, \chi)$ is infinite, and it has only a simple pole, so the product $P(s)$ will have at least a first-order 0 at $s = 1$. Since P does not have a pole at 1, it is continuous there. But we have already seen that $P(s) \geq 1$ arbitrarily close to $s = 1$, so we have a contradiction. To prove that $L(1, \chi) \neq 0$, all that remains for us to show is that $L(s, \chi)$ is not uniformly zero on $Re(s) > 0$. But this is obvious: $L(s, \chi) = 1 + \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s}$. By choosing $\Re(s)$ arbitrarily large, we can make the absolute value of the infinite sum arbitrarily small. In particular, we can make it smaller than 1, so that $L(s, \chi) \geq 1 - \left| \sum_{n=2}^{\infty} \frac{\chi(n)}{n^s} \right| > 0$.

Note that since $L(s,\chi)$ is meromorphic at $s=1$, the fact that it is nonzero at 1 implies that it is nonzero in a neighborhood of 1. Now that we have proved the two key properties of Dirichlet L-series, we are ready to move on to the main proof of the theorem.

4 The Proof

We will actually prove a slightly stronger version of Dirichlet's Theorem than the one stated at the beginning of the paper. In particular, we will show that there are "equally many" primes $p \equiv a \pmod b$ for each $a \in (\mathbf{Z}/b\mathbf{Z})^*$. To make this statement more exact, we will introduce the idea of *Dirichlet densities.*

Definition: The Dirichlet density of some subset S of the prime numbers is

$$\lim_{s\to 1^+}\left(\frac{\sum_{p\in S} p^{-s}}{\sum_p p^{-s}}\right), \tag{7}$$

assuming that this limit exists.

We will show each set $S_a \equiv \{\text{primes } p \mid p \equiv a \pmod b\}$ has Dirichlet density $\frac{1}{\phi(b)}$, or, equivalently, that

$$\lim_{s\to 1^+}\left(\sum_{p\equiv a \pmod b}\frac{1}{p^s} - \frac{1}{\phi(b)}\sum_p \frac{1}{p^s}\right) \tag{8}$$

is finite. Assuming that the second sum diverges as $s \to 1$, the only way the difference can be finite is if there are an infinite number of terms in the first sum, i.e., there are infinitely many primes $p \equiv a \pmod b$.

Proposition: $\sum_p \frac{1}{p^s}$ *diverges as* $s \to 1^+$.

Proof: We will take s to be real. For each prime p, consider

$$\begin{aligned}\left|\frac{1}{p^s}+\ln\left(1-\frac{1}{p^s}\right)\right| &= \left|\frac{1}{p^s}-\sum_{n=1}^{\infty}\frac{1}{np^{ns}}\right| \\ &= \sum_{n=2}^{\infty}\frac{1}{np^{ns}}\end{aligned}$$

$$
\begin{aligned}
&< \frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{p^{ns}} \\
&\leq \frac{1}{2}\sum_{n=2}^{\infty}\frac{1}{p^{n}} \\
&= \frac{1}{2}p^{-2}\frac{1}{1-p^{-1}} \\
&= \frac{1}{2p(p-1)} \\
&\leq \frac{1}{p^2}.
\end{aligned}
$$

Since $\sum_p \frac{1}{p^2} < \sum_{n=1}^{\infty} \frac{1}{n^2}$ converges absolutely, it follows that $\lim_{s\to 1^+} \sum_p \left(\frac{1}{p^s} + \ln\left(1 - \frac{1}{p^s}\right)\right)$ also converges absolutely. Now suppose that $\lim_{s\to 1^+} \sum_p \frac{1}{p^s}$ exists. Since s is real, each term is positive, so the sum conveges absolutely. Thus it follows that

$$\lim_{s\to 1^+}\sum_p \left(\frac{1}{p^s} + \ln\left(1-\frac{1}{p^s}\right)\right) - \lim_{s\to 1^+}\sum_p \frac{1}{p^s} = \lim_{s\to 1^+}\sum_p \ln\left(1-\frac{1}{p^s}\right).$$

In particular, the limit on the right-hand side must converge to the difference of the limits on the left-hand side. The exponential of the right-hand side, $\lim_{s\to 1^+}\prod_p \left(1-\frac{1}{p^s}\right)$, must therefore have a finite *non-zero* value. But then $\lim_{s\to 1^+}\zeta(s) = \left(\lim_{s\to 1^+}\prod_p \left(1-\frac{1}{p^s}\right)\right)^{-1}$ would have a finite value. (Notice that we have pulled the limit sign out of an exponent and inside an inverse in the last two step, as we are allowed to do if the limit exists.) We know that $\zeta(s)$ has a pole at 1, so it must be that $\sum_p \frac{1}{p^s}$ diverges as $s \to 1^+$.

We will now show that the limit in (8) is finite. For s with $\Re(s) > 1$, consider

$$
\begin{aligned}
\sum_{\chi\in\hat{G}} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} &= \sum_p \frac{\sum_{\chi\in\hat{G}}\chi(a^{-1}p)}{p^s} && (9) \\
&= \sum_{p\equiv a \pmod b} \frac{\phi(b)}{p^s} && (10) \\
&= \phi(b) \sum_{p\equiv a \pmod b} \frac{1}{p^s}. && (11)
\end{aligned}
$$

We were able to switch the order of the sums in (9) because $\sum_p \frac{\chi(p)}{p^s}$ is absolutely convergent for $\Re(s) > 1$. We can rewrite the left-hand side of the equation by removing the trivial character from the sum:

$$\begin{aligned}\sum_{\chi \in \hat{G}} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} &= \chi_0(a^{-1}) \sum_p \frac{\chi_0(p)}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s} \quad (12)\\ &= \sum_p \frac{1}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s}. \quad (13)\end{aligned}$$

Combining (11) and (13), we have

$$\phi(b) \sum_{p \equiv a \pmod b} \frac{1}{p^s} = \sum_p \frac{1}{p^s} + \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s},$$

which we can rewrite as

$$\sum_{p \equiv a \pmod b} \frac{1}{p^s} - \frac{1}{\phi(b)} \sum_p \frac{1}{p^s} = \frac{1}{\phi(b)} \sum_{\chi \neq \chi_0} \chi(a^{-1}) \sum_p \frac{\chi(p)}{p^s}. \quad (14)$$

The left-hand side is the argument of the limit in (8), so we can complete our proof of Dirichlet's Theorem by showing that the right-hand side has a finite limit as $s \to 1^+$. There are a finite number of characters χ, so all we have to show is that for all $\chi \neq \chi_0$, the infinite sum $\sum_p \frac{\chi(p)}{p^s}$ converges as $s \to 1^+$.

Proposition: $\sum_p \frac{\chi(p)}{p^s}$ *converges as* $s \to 1^+$ *for all* $\chi \neq \chi_0$.

Proof: We will proceed by showing that the sum differs from $\ln(L(s,\chi))$ by an analytic function in a neighborhood around 1. (Since $L(s, \chi \neq \chi_0)$ is analytic for $s > 0$ and $L(s,\chi) \neq 0$ near 1, it follows that $\ln(L(s,\chi))$ is analytic near 1, and therefore so is its sum with any analytic function.) The proof is similar to the one showing that $\sum_p \frac{1}{p^s}$ diverges as $s \to 1^+$.

$$\begin{aligned}\ln(L(s,\chi)) - \sum_p \frac{\chi(p)}{p^s} &= \ln\left(\prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}\right) - \sum_p \frac{\chi(p)}{p^s}\\ &= \sum_p \left(-\ln\left(1 - \frac{\chi(p)}{p^s}\right) - \frac{\chi(p)}{p^s}\right)\\ &= \sum_p \left(\sum_{n=1}^{\infty} \frac{\chi^n(p)}{np^{ns}} - \frac{\chi(p)}{p^s}\right)\end{aligned}$$

$$= \sum_p \sum_{n=2}^{\infty} \frac{\chi^n(p)}{np^{ns}}.$$

This series is absolutely convergent in the region $\Re(s) > 1/2$:

$$\begin{aligned}
\sum_p \sum_{n=2}^{\infty} \left| \frac{\chi^n(p)}{np^{ns}} \right| &= \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n\Re(s)}} \\
&< \frac{1}{2} \sum_p \sum_{n=2}^{\infty} p^{-n\Re(s)} \\
&= \frac{1}{2} \sum_p p^{-2\Re(s)} \frac{1}{1 - p^{-\Re(s)}} \\
&= \frac{1}{2} \sum_p \frac{1}{p^{\Re(s)}(p^{\Re(s)} - 1)}
\end{aligned}$$

which converges (since the terms decrease like $1/p^{2\Re(s)}$, and $2\Re(s) > 1$), completing the proof of Dirichlet's Theorem.

5 The Chebotarev Density Theorem

The following is a generalization of Dirichlet's Theorem:
Chebotarev's Density Theorem: Let L be a Galois extension of number field K, and for $\sigma \in Gal(L/K)$ define C_σ to be the conjugacy class of σ. Let S be the set of prime ideals $\mathfrak{p}$ of K such that for every prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$, the Frobenius element of $\mathfrak{P}$ is in C_σ. Then S has Dirichlet density $\frac{|C_\sigma|}{|Gal(L/K)|}$.

To see how Dirichlet's Theorem follows, let $K = \mathbf{Q}$ and let $L = \mathbf{Q}(\zeta_b)$, where ζ_b is one of the primitive b^{th} roots of unity. $\mathbf{Q}(\zeta_b)$ is an Abelian extension of $\mathbf{Q}$ with Galois group $(\mathbf{Z}/b\mathbf{Z})^*$, so $C_\sigma = \{\sigma\}$ for all $\sigma \in \text{Gal}(\mathbf{Q}(\zeta_b)/\mathbf{Q})$, and the Frobenius element of $\mathfrak{P}$ is just the Artin symbol $\left(\frac{\mathbf{Q}(\zeta_b)/\mathbf{Q}}{p}\right) = \bar{p} \in (\mathbf{Z}/b\mathbf{Z})^*$ for all $\mathfrak{P}$ lying over any prime p that does not divide b. Thus we see that there is a bijective correspondence between the conjugacy classes mod b of primes that do not divide b and the elements of the Galois group, so that the set S in the statement of the theorem becomes $S_a = \{\text{primes } p \in \mathbf{Z} \mid p \equiv a \pmod{b}\}$. Since $|C_\sigma| = 1$ and $|\text{Gal}(\mathbf{Q}(\zeta_b)/\mathbf{Q})| = \phi(b)$, the theorem tells us that the set S_a has density $\frac{1}{\phi(b)}$ for each $a \in (\mathbf{Z}/b\mathbf{Z})^*$, which is exactly what we showed in proving Dirichlet's Theorem.

6 Computation

The form of Dirichlet's Theorem that we have proved tells us that, on average, one of every $\phi(b)$ primes will be congruent to $a \pmod{b}$. It is possible, however, that for a given a, b, the distribution of primes will be very uneven; the theorem does not guarantee that, say, one of the first $\phi(b)$ primes that do not divide b will be congruent to a. We can, however, find experimentally how long it takes to find a prime $p \equiv a \pmod{b}$ for various a, b. The following MAGMA code will find the first prime $p = a + nb$ for $0 \leq n \leq c$, or return -1 if there is no such prime, i.e., if our choice of c is too small. (It will return 0 if we have entered inappropriate values for a, b, or c.)

```
findp:=function(a,b,c)
if not (IsIntegral(a) and IsIntegral(b) and IsIntegral(c)) then
return 0;
end if;
if ((a le 0) or (c le 0) or (b le 1)) then
return 0;
end if;
if Gcd(a,b) ne 1 then
return 0;
end if;
if Gcd(a,b) eq 1 then
x:=-1;
for n in [0..c] do
if IsPrime(a+n*b) then
x:=n;
return [n,a+n*b];
end if;
end for;
return x;
end if;
end function;
```

Using this function, one can then easily write a double for-loop to check a desired range of values for a and b. (In doing this, one may wish to change the function so that it will return a and b along with n and $a + nb$.) For $a, b \leq 20$, we find that there is always a prime $p = a + nb$ with $n \leq 10$, and the only choice for which we have to go out to $n = 10$ is $a = 1$, $b = 19$. For

$b = 100$, the largest value of n for any a is 4. For $b = 97$ (a prime), the highest n is 15. If we set $a = 1$ and let b range over the integers less than 100, the highest n is 12. For $100 \leq b \leq 110$, $30 \leq a \leq 40$ (to choose an arbitrary range of values), the largest value of n is 14. From these examples, it seems that n will generally not be larger $\phi(b)$, from which we can guess that the primes $p \equiv a \pmod{b}$ are fairly evenly distributed.