Course 428 — Sample Paper 2

Timothy Murphy

24 April 2006

Credit will be given for the best 6 questions answered. Logarithmic tables will be available.

1. Show that if $a, b \in \mathbb{Z}$ and $\gcd(a, b) = d$ then there exist $u, v \in \mathbb{Z}$ such that
$$au + bv = d.$$
Show that if $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and $r, s \in \mathbb{Z}$ then there is an $x \in \mathbb{Z}$ such that
$$x \equiv r \bmod m, \quad x \equiv s \bmod n.$$
What is the smallest integer $x > 0$ such that
$$x \equiv 3 \bmod 28, \quad x \equiv 5 \bmod 101?$$

Answer:

(a) *Consider the set S of integers of the form*
$$au + bv \quad (u, v \in \mathbb{Z}).$$
Let d be the smallest integer > 0 in S. We claim that
$$d = \gcd(a, b).$$
Firstly,
$$d \mid a;$$
for otherwise we could divide a by d,
$$a = qd + r,$$
with $0 < r < d$, and then $r \in S$, contradicting the minimality of d.

Similarly

$$d \mid b.$$

Conversely,

$$e \mid a, b \implies e \mid d.$$

Hence

$$d = \gcd(a, b),$$

and the result follows.

[For an alternative proof, carry out the Euclidean algorithm to compute $\gcd(a, b)$*:*

$$\begin{aligned} a &= bq_1 + r_1, \quad (0 < r_1 < b), \\ b &= r_1 q_2 + r_2, \quad (0 < r_2 < r_1), \\ r_1 &= r_2 q_3 + r_3, \quad (0 < r_3 < r_2), \end{aligned}$$

until finally

$$r_{n-1} = r_n q_{n+1},$$

with $r_{n+1} = 0$*.*
Then it follows, working backwards, that

$$r_n = \gcd(a, b).$$

It also follows, working backwards, that r_n *can be expressed in the form*

$$r_n = r_{i-1} u_i + r_i v_i$$

with $u_i, v_i \in \mathbb{Z}$*; and so, finally,*

$$r_n = au + bv.]$$

(b) *Consider the map*

$$\Theta : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

under which

$$r \bmod mn \mapsto (r \bmod m, r \bmod n).$$

This map is injective. For suppose

$$r \bmod m = s \bmod m, \; r \bmod n = s \bmod n,$$

ie

$$m \mid r - s, \ n \mid r - s.$$

Then

$$mn \mid r - s,$$

since $\gcd(m, n) = 1$, *ie*

$$r \bmod mn = s \bmod mn.$$

But each of the two sets $\mathbb{Z}/(mn)$ *and* $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ *contains mn elements. Hence*

$$\Theta \text{ injective} \implies \Theta \text{ surjective}.$$

In other words, given any $r, s \in \mathbb{Z}$ *we can find* $x \in \mathbb{Z}$ *such that*

$$\Theta(x) = (r, s),$$

ie

$$x \bmod m = r, \ x \bmod n = s.$$

(c) *Let us use the Euclidean Algorithm (slightly modified, to allow negative remainders) to determine* $\gcd(28, 101)$*:*

$$\begin{aligned} 101 &= 28 \cdot 4 - 11, \\ 28 &= 11 \cdot 3 - 5, \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

Thus $\gcd(28, 101) = 1$ *(as is obvious anyway by factoring); and working backwards,*

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2(3 \cdot 11 - 28) \\ &= 2 \cdot 28 - 5 \cdot 11 \\ &= 2 \cdot 28 - 5(4 \cdot 28 - 101) \\ &= 5 \cdot 101 - 18 \cdot 28. \end{aligned}$$

Thus

$$5 \cdot 101 \equiv 1 \bmod 28, \quad 18 \cdot 28 \equiv -1 \bmod 101.$$

It follows that

$$n = 3 \cdot 5 \cdot 101 - 5 \cdot 18 \cdot 28$$

satisfies

$$n \equiv 3 \bmod 28, \quad n \equiv 5 \bmod 101.$$

The general solution of these simultaneous congruences will be

$$m = n + 28 \cdot 101\, q$$

with $q \in \mathbb{Z}$*.*
We have to choose q *so that*

$$0 \le m < \cdot 28 \cdot 101,$$

ie

$$m = \left[\frac{n}{28 \cdot 101}\right].$$

Computing,

$$\begin{aligned} n &= 15 \times 101 - 90 \cdot 28 \\ &= 1515 - 2520 \\ &= -1005 \end{aligned}$$

Hence

$$\begin{aligned} m &= 28 \cdot 101 - 1005 \\ &= 2828 - 1005 \\ &= 1823. \end{aligned}$$

[Of course any method of arriving at this result would be valid.]

2. Show that if $2^m + 1$ is prime then $m = 2^n$ for some $n \in \mathbb{N}$.

   Show that the Fermat number

   $$F_n = 2^{2^n} + 1,$$

   where $n > 0$, is prime if and only if

   $$3^{2^{2^n - 1}} \equiv -1 \bmod F_n.$$

   Use this test to determine the primality of F_3.

   Answer:

(a) *If r is odd then*

$$x+1 \mid x^r+1.$$

Thus if m contains an odd factor r, say $m = rs$, then

$$2^s+1 | 2^{rs}+1.$$

It follows that if 2^m+1 is prime then m has no odd factors, ie $m = 2^n$ for some n.

(b) *Suppose F_n is prime.*

We assume the following result.

Lemma 2.1. *If p is an odd prime then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$$

for any a coprime to p.

Applying this with $p = F_n$,

$$3^{2^{2^n}-1} \equiv \left(\frac{3}{p}\right) \bmod p.$$

Since

$$F_n \equiv 1 \bmod 5$$

it follows by Gauss' Recipricity Law that

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

But

$$2^{2^n} \equiv 1 \bmod 3$$

(since $3^2 \equiv 1$),

$$p = F_n \equiv 2 \bmod 3.$$

Thus

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

It follows that

$$3^{2^{2^n-1}} \equiv -1 \bmod p.$$

(c) *Conversely, suppose*

$$3^{2^{2^n-1}} \equiv -1 \bmod F_n.$$

Suppose F_n *is composite, say*

$$F_n = qr,$$

where q *is prime. Then*

$$3^{2^{2^n-1}} \equiv -1 \bmod q.$$

It follows that the order of $3 \bmod q$ *is* 2^{2^n}. *But we know that*

$$3^{q-1} \equiv 1 \bmod q.$$

It follows that

$$2^{2^n} \mid q-1,$$

ie

$$F_n - 1 \mid q-1,$$

which is impossible since $q < F_n$,

(d) *Since*

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257,$$

we must compute

$$3^{2^7} = 3^{128} \bmod 257.$$

We know that the order of $3 \bmod ; 257$ *divides 256, ie it is a power of 2. And*

$$3^{256} \equiv 1 \bmod 257 \implies 3^{128} \equiv \pm 1 \bmod 257;$$

while

$$3^{128} \equiv 1 \bmod 257 \iff 3^{64} \equiv \pm 1 \bmod 257.$$

We have to show that this is not the case.
Now

$$3^5 = 3 \cdot 81 = 243.$$

Thus

$$3^5 \equiv -14 \bmod 257.$$

Hence

$$3^{10} \equiv 14^2 = 196 \equiv -61 \bmod 257,$$

and so

$$3^{12} \equiv -9 \cdot 61 = -549 \equiv -35 \bmod 257.$$

Thus

$$3^{14} \equiv -315 \equiv 58 \bmod 257,$$

and

$$3^{16} \equiv 522 \equiv 8 = 2^3 \bmod 257,$$

Hence

$$3^{32} \equiv 2^6 \bmod 257,$$

and so

$$3^{64} \equiv 2^{12} = 4096 = 4 \cdot 1024 \equiv 4 \cdot -4 = -16 \bmod 257.$$

So

$$3^{128} \equiv 16^2 \equiv -1 \bmod 257,$$

and we conclude that F_3 is prime.

3. Define the Jacobi symbol $\left(\dfrac{m}{n}\right)$ for $m \in \mathbb{N}$, $n \in \mathbb{Z}$ with m odd. Assuming Gauss' Law of Quadratic Reciprocity, show that if $m, n \in \mathbb{N}$ are both odd then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Prove that the odd number $n \in N$ is prime if and only if

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$$

for all a coprime to n.

Answer:

(a) If

$$m = p_1 \cdots p_r, \quad n = q_1 \cdots q_s,$$

with p_i, q_j prime, then the Jacobi symbol is defined by

$$\left(\frac{m}{n}\right) = \prod_{1 \le i \le r,\ 1 \le j \le s} \left(\frac{p_i}{q_j}\right).$$

(b) Gauss' Law states that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

It follows that

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j}\left(\frac{p_i-1}{2}\frac{q_j-1}{2}\right).$$

Lemma 3.1. *If u, v are odd then*

$$\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \bmod 2.$$

Proof. If u, v are odd then

$$(u-1)(v-1) \equiv 0 \bmod 4,$$

ie

$$(uv-1) \equiv (u-1) + (v-1) \bmod 4,$$

or

$$\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \bmod 2.$$

which is evident. □

Repeated application of this Lemma gives

$$\frac{m-1}{2} \equiv \sum_i \frac{p_i-1}{2},$$
$$\frac{n-1}{2} \equiv \sum_j \frac{q_j-1}{2}.$$

Multiplying these together,

$$\begin{aligned}\frac{m-1}{2}\frac{n-1}{2} &= \sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}\\ &= \left(\frac{m}{n}\right)\left(\frac{n}{m}\right).\end{aligned}$$

(c) *Suppose n is prime. Then*

$$a^{n-1} \equiv 1 \bmod n \implies a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n.$$

Suppose $\left(\frac{a}{n}\right) = 1$. *Then*

$$a \equiv b^2 \implies a^{\frac{n-1}{2}} \equiv b^{n-1} \equiv 1 \bmod n.$$

Now the equation

$$x^{\frac{n-1}{2}} = 1$$

in the finite field $\mathbb{F}_n = \mathbb{Z}/(n)$ *has at most* $(n-1)/2$ *roots. But there are* $(n-1)/2$ *quadratic residues. Hence*

$$a^{\frac{n-1}{2}} \equiv 1 \bmod n \iff \left(\frac{a}{n}\right) = 1.$$

Conversely, suppose this holds for all a coprime to n; and suppose n is not prime.

Then n must be square-free. For suppose

$$n = p^e q,$$

where p is prime and $gcd(p, q) = 1$.

By hypothesis

$$a^{n-1} \equiv 1 \bmod n$$

for all a coprime to n. Hence

$$a^{n-1} \equiv 1 \bmod p^e,$$

ie the order of $a \bmod p^e$ *divides* $n-1$.

Since $\phi(p^e) = p^{e-1}(p-1)$, *the order of*

$$a \in (\mathbb{Z}/p^e)^\times$$

divides $p^{e-1}(p-1)$; *and it is easy to see that there are elements whose order is divisible by p, eg* $a = 1 + p$ *is such an element, since*

$$a^{p-1} \equiv 1 + (p-1)p \equiv 1 - p \bmod p^2,$$

so the order of a does not divide $p - 1$.

By the Chinese Remainder Theorem we can find a such that

$$a \equiv 1 + p \bmod p^e, \; a \equiv 1 \bmod q.$$

Then a is coprime to n, and p divides the order of $a \bmod n$. *Hence*

$$p \mid n - 1,$$

which is absurd.

Thus

$$n = p_1 p_2 \cdots p_r,$$

with distinct primes p_i.

We can certainly find an a with

$$\left(\frac{a}{n}\right) = -1,$$

eg by the Chinese Remainder Theorem we can find a such that a is a quadratic non-residue $\bmod p_1$ *and a quadratic residue modulo the other p_i. Then*

$$a^{\frac{n-1}{2}} \equiv -1 \bmod n,$$

and so

$$a^{\frac{n-1}{2}} \equiv -1 \bmod p_i$$

for each i.

Suppose

$$2^e \parallel n - 1,$$

ie $2^e \mid n-1$ *but* $2^{e+1} \nmid n-1$. *[In other words,*

$$n - 1 = 2^e m,$$

where m is odd. Note that in the following argument, we are only concerned with the power of 2 dividing the order of an element; if you like we are concerned with the 2-adic value of the order.]

Then the order of $a \bmod n$ *is divisible by* 2^e*; hence the order of* $a \bmod p_i$ *is also divisible by* 2^e. *Thus*

$$2^e \mid p_i - 1,$$

ie

$$p_i \equiv 1 \bmod 2^e$$

for each i.

But now choose a so that it is a quadratic non-residue mod p_1 *and* mod p_2 *but a quadratic residue modulo the other p_i. Then*

$$\left(\frac{a}{n}\right) = (-1)(-1)1 \cdots 1 = 1.$$

Hence

$$a^{\frac{n-1}{2}} \equiv 1 \bmod n,$$

and so

$$a^{\frac{n-1}{2}} \equiv 1 \bmod p.$$

Thus if

$$2^f \parallel \text{order}(a \bmod p)$$

then

$$f \leq e - 1;$$

while on the other hand, since $2^e \mid p - 1$,

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p \implies f \geq e.$$

We conclude that n must be prime.

Remarks:

(a) *I've removed the part of this question which read:*

> *Apply this test to determine the primality (or otherwise) of 10013.*

I think I gave this question as homework in an earlier year when the course covered computer methods for primality testing and factorisation. I guess I expected the student to write a computer program to solve this question. I certainly don't see any way of solving it 'by hand' in the time available in an exam!

Running the program `/usr/games/factor` 10013 on the Maths computer system tells me that

$$10013 = 17 \cdot 19 \cdot 31.$$

Recall that if p *is an odd prime then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8, \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

Since

$$10013 \equiv 5 \equiv -3 \bmod 8$$

it follows that

$$\left(\frac{2}{10013}\right) = -1.$$

Thus if $n = 10013$ *is prime then*

$$2^{5006} \equiv -1 \bmod 10013.$$

It is easy to compute this, knowing the factorisation of n.
The order of $2 \bmod 17$ *is 5 since*

$$2^4 = 16 \equiv -1 \bmod 17.$$

The order of $2 \bmod 31$ *is 5 since*

$$2^5 = 32 \equiv 1 \bmod 31.$$

It remains to compute the order of $2 \bmod 19$. *This order divides* $19 - 1 = 18$. *Since it is not 2 or 3, it must be 6, 9 or 18.*
We have

$$2^6 = 64 \equiv 7 \bmod 19.$$

Hence

$$2^9 \equiv 8 \cdot 7 = 56 \equiv -1 \bmod 19.$$

Thus the order of $2 \bmod 19$ *is 18.*
Since

$$5006 \bmod 5 = 1, \quad 5006 \bmod 18 = 2,$$

it follows that

$$2^{5006} \begin{cases} \equiv 1 \bmod 17, \\ \equiv 2 \bmod 19, \\ \equiv 1 \bmod 31. \end{cases}$$

So certainly

$$2^{5006} \not\equiv -1 \bmod 10013.$$

In fact this argument shows that

$$2^{10012} \begin{cases} \equiv 1 \bmod 17, \\ \equiv 4 \bmod 19, \\ \equiv 1 \bmod 31. \end{cases}$$

So

$$2^{10012} \not\equiv 1 \bmod 10013,$$

and 10013 fails even Fermat's primality test.

(b) *The method suggested in the question is a perfectly sensible probabilistic primality test, since it is easy to compute* $\left(\frac{a}{n}\right)$ *using the generalised Reciprocity Law given earlier in the question. It could be used as an alternative to the standard Miller-Rabin probabilistic primality test.*

Let us recall the Miller-Rabin test for the primality of n.

Let

$$n - 1 = 2^e m,$$

where m *is odd.*

If n *is prime then*

$$a^{2^e m} \equiv 1 \bmod n \implies a^{2^{e-1} m} \equiv \pm 1 \bmod n.$$

If now

$$a^{2^{e-1} m} \equiv 1 \bmod n$$

then

$$a^{2^{e-2} m} \equiv \pm 1 \bmod n.$$

Continuing in this way, we conclude that if $\gcd(a, n) = 1$ *then either*

$$a^{2^f m} \equiv -1 \bmod n$$

for some $f \in [0, e-1]$, *or else*

$$a^m \equiv 1 \bmod n.$$

Conversely, if this is true for all a coprime to n then n must be prime.

The proof is very similar to that in the question, and depends in the same way on the power of 2 dividing the order of a modulo different numbers. To simplify the discussion, let us write

$$v(a, n) = e$$

if the order of $a \bmod n$ *is* r *and*

$$2^e \parallel r.$$

It is not difficult to see that

$$a^{2^f m} \equiv -1 \bmod n \iff v(a, n) = f + 1.$$

But if $p \mid n$ *then*

$$a^{2^f m} \equiv -1 \bmod n \implies a^{2^f m} \equiv -1 \bmod p \implies v(a, p) = f + 1.$$

Thus

$$v(a, p) = v(a, n)$$

if $p \mid n$*. In particular,* $v(a, p)$ *is the same for all primes dividing* n*.*

But it is easy to see that this cannot be the case if two distinct primes $p, q \mid n$*.*

For by the Chinese Remainder Theorem we can find a *which is a quadratic residue* $\bmod p$ *and a quadratic non-residue* $\bmod q$*. Then*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p, \quad a^{\frac{q-1}{2}} \equiv -1 \bmod q.$$

On the other hand, we can find b *which is a quadratic non-residue* $\bmod p$ *and a quadratic residue* $\bmod q$*. Then*

$$b^{\frac{p-1}{2}} \equiv -1 \bmod p, \quad b^{\frac{q-1}{2}} \equiv 1 \bmod q.$$

But it follows from these that

$$v(a, p) < v(b, p), \quad v(a, q) > v(b, q),$$

which is clearly incompatible with

$$v(a, p) = v(a, q), \quad v(b, p) = v(b, q).$$

It only remains to deal with the case

$$n = p^e.$$

But as we saw in our proof, it is easy to find a *in this case such that*

$$a^{n-1} \not\equiv 1 \bmod n.$$

4. Show that every irrational number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ has an infinity of rational approximations x/y with

$$|\alpha - \frac{x}{y}| < \frac{1}{y^2}.$$

Find five such approximations for $\sqrt{2}$.

Suppose $m > 1$ is square-free. Show that the equation

$$x^2 - my^2 = 1$$

has an infinity of solutions.

Answer:

(a) *Choose any integer $N > 0$, and consider the remainders*

$$\{0\alpha\},\ \{1\alpha\},\ \{2\alpha\}, \dots \{N\alpha\},$$

where

$$\{x\} = x - [x].$$

These $N + 1$ numbers lie in the interval $[0, 1)$. Let us divide this interval into N equal parts

$$[0, 1/N),\ [1/N, 2/N), \dots, [(N-1)/N, 1).$$

Two of the remainders, say $\{r\alpha\}$, $\{s\alpha\}$ with $r < s$, must fall into the same sub-interval.

But then

$$|\{s\alpha\} - \{r\alpha\}| < \frac{1}{N}.$$

In other words,

$$|s\alpha - [s\alpha] - (r\alpha - [r\alpha])| < \frac{1}{N}.$$

On setting

$$x = [s\alpha] - [r\alpha], \quad y = s - r,$$

this can be written

$$|y\alpha - x| < \frac{1}{N},$$

from which the result follows since

$$y \leq N.$$

(b) We can get approximants to $\sqrt{2}$ *from its continued fraction:*

$$\sqrt{2} = 1 + (\sqrt{2} - 1),$$

and

$$\begin{aligned} \frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1 \\ &= 2 + (\sqrt{2} - 1). \end{aligned}$$

Thus

$$\sqrt{2} = [1, 2, 2, 2, \dots].$$

The approximants are

$$\frac{p_n}{q_n}$$

where

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2},$$

with

$$p_0 = a_0 = 1,\ q_0 = 1, \quad p_1 = a_0 a_1 + 1 = 2,\ q_1 = a_1 = 1.$$

The first 6 approximants are

$$\begin{aligned} &\frac{1}{1}, \\ &\frac{2}{1}, \\ &\frac{2 \cdot 2 + 1}{2 \cdot 1 + 1} = \frac{5}{3}, \\ &\frac{2 \cdot 5 + 2}{2 \cdot 3 + 1} = \frac{12}{7}, \\ &\frac{2 \cdot 12 + 5}{2 \cdot 7 + 3} = \frac{29}{17}, \\ &\frac{2 \cdot 29 + 12}{2 \cdot 17 + 7} = \frac{70}{41}. \end{aligned}$$

These all satisfy

$$\begin{aligned} |\alpha - \frac{p_n}{q_n}| &< \frac{1}{q_n q_{n+1}} \\ &< \frac{1}{q_n^2}. \end{aligned}$$

(c) Here is an alternative solution to Pell's equation

$$x^2 - my^2 = 1$$

based on the fact that the continued fraction for $\sqrt{m}$ *is periodic: say*

$$\sqrt{m} = [a_0, \ldots, a_{\ell-1}, \dot{a_n}, \ldots, \dot{a_{n+k}}],$$

ie the continued fraction for $\sqrt{m}$ *starts with an initial sequence of length* ℓ*, followed by a repeated sequence of length* k*.*

Let p_n/q_n *be the successive approximants, so that*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2};$$

and let

$$\alpha_n = [a_n, a_{n+1}, \ldots],$$

so that

$$\sqrt{m} = [a_0, ..., a_{n-1}, \alpha_n] = \frac{u_n}{v_n},$$

where

$$u_n = \alpha_n p_{n-1} + p_{n-2}, \quad v_n = \alpha_n q_{n-1} + q_{n-2}.$$

Then

$$\alpha_n = \alpha_{n+k}$$

if $n \geq \ell$*, or more generally*

$$\alpha_n = \alpha_{n+kj}$$

for $j \geq 0$*.*

We know that

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^n.$$

[This is readily proved by induction on n.] Thus if we set

$$M_n = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}$$

then

$$\det M_n = (-1)^{n-1}.$$

In particular M_n *is unimodular, ie its inverse is also an integer matrix.*

Now

$$M_n \begin{pmatrix} \sqrt{m} \\ 1 \end{pmatrix} = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

Since

$$\alpha_{n+k} = \alpha_n$$

if $n \geq \ell$,

$$u_{n+k}/v_{n+k} = u_n/v_n$$

Thus

$$\begin{pmatrix} u_{n+k} \\ v_{n+k} \end{pmatrix} = \lambda \begin{pmatrix} u_n \\ v_n \end{pmatrix}$$

for some λ.
It follows that

$$M_{n+k} \begin{pmatrix} \sqrt{m} \\ 1 \end{pmatrix} = \lambda\, M_n \begin{pmatrix} \sqrt{m} \\ 1 \end{pmatrix}.$$

Hence if we set

$$M = M_n^{-1} M_{n+k} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then

$$M \begin{pmatrix} \sqrt{m} \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} \sqrt{m} \\ 1 \end{pmatrix},$$

ie

$$a\sqrt{m} + b = \lambda\sqrt{m}, \quad c\sqrt{m} + d = \lambda.$$

Eliminating λ,

$$a\sqrt{m} + b = \sqrt{m}(c\sqrt{m} + d),$$

ie

$$(b - cm) + (a - d)\sqrt{m} = 0.$$

Thus

$$b = cm,\ a = d.$$

But

$$\det M = ad - bc = \pm 1,$$

according as k *is even or odd; and so*

$$a^2 - mb^2 = \pm 1.$$

Since we can replace k *by* kj, *this gives a solution — in fact an infinity of solutions — of Pell's equation*

$$x^2 - my^2 = 1.$$

5. Determine the ring A of integers in the field $\mathbb{Q}(\sqrt{5})$, and show that the Fundamental Theorem of Arithmetic holds in this ring.

The Fibonacci numbers u_i are defined by the recursion relation

$$u_0 = 0,\ u_1 = 1,\ u_{i+1} = u_i + u_{i-1}.$$

Suppose $p \neq 5$ is a prime number. Show that

$$p \mid u_{p-1} \text{ if } p \equiv \pm 1 \bmod 5,$$

while

$$p \mid u_{p+1} \text{ if } p \equiv \pm 2 \bmod 5,$$

Answer:

(a) *We assume the following result.*

Lemma 5.1. *The algebraic number α is an algebraic integer if and only if its minimal polynomial $m(x)$ over $\mathbb{Q}$ has integer coefficients.*

Suppose

$$\alpha = u + v\sqrt{5} \in \bar{\mathbb{Z}}$$

where $u, v \in \mathbb{Q}$.
Then α satisfies the equation

$$(x - u)^2 = 5v^2,$$

ie

$$f(x) = x^2 - 2ux + (u^2 - 5v^2) = 0.$$

If $v = 0$ then the minimal polynomial of α is

$$m(x) = x - u;$$

so $\alpha \in \bar{\mathbb{Z}}$ if and only if $u \in \mathbb{Z}$.
If $v \neq 0$ then $f(x)$ must be the minimal polynomial of α. Thus

$$\alpha \in \bar{\mathbb{Z}} \iff 2u,\ u^2 - 5v^2 \in \mathbb{Z}.$$

Hence

$$u = \frac{a}{2},$$

with $a \in \mathbb{Z}$. *Also*

$$5v^2 - \frac{a^2}{4} \in \mathbb{Z},$$

and so

$$5v^2 = \frac{c}{4},$$

with $c \in \mathbb{Z}$. *It follows that*

$$v = \frac{b}{2}$$

with $b \in \mathbb{Z}$.

But now

$$u^2 - 5v^2 = \frac{a^2 - 5b^2}{4}.$$

Thus

$$a^2 - 5v^2 \equiv 0 \bmod 4.$$

Since

$$n^2 \equiv 0 \text{ or } 1 \bmod 4,$$

this holds if and only if a, b *are both odd or both even.*

We conclude that the integers in $\mathbb{Q}(\sqrt{5})$ *are the numbers of the form*

$$\frac{a + b\sqrt{5}}{2},$$

where $a, b \in \mathbb{Z}$ *and* $a \equiv b \bmod 2$.

In other words, the integers are the numbers

$$m + n\theta \quad (m, n \in \mathbb{Z})$$

where

$$\theta = \frac{1 + \sqrt{5}}{2}.$$

6. Define an *ideal* $\mathfrak{a}$ in a commutative ring A.

   What is meant by saying that $\mathfrak{a}$ is *prime*?

   Show that a maximal ideal is necessarily prime. Does the converse hold?

   Sketch the proof that in a number ring every ideal is a product of prime ideals, unique up to order.

   Answer:

(a) *An ideal* $\mathfrak{a} \subset A$ *is a non-empty subset such that*

   i. $a, b \in \mathfrak{a} \implies a + b \in \mathfrak{a}$;

   ii. $a \in A,\ b \in \mathfrak{a} \implies ab \in \mathfrak{a}$.

(b) *The ideal* $\mathfrak{a} \neq A$ *is prime if*

$$ab \in \mathfrak{a} \implies a \in \mathfrak{a} textor b \in \mathfrak{a}.$$

[An alternative, equivalent, definition is: The ideal $\mathfrak{p} \neq A$ *is prime if*

$$\mathfrak{ab} \subset \mathfrak{p} \implies \mathfrak{a} \subset \mathfrak{p} \text{ or } \mathfrak{b} \subset \mathfrak{p}$$

for any two ideals $\mathfrak{a}, \mathfrak{b} \subset A$*.]*

(c) *Suppose the ideal* $\mathfrak{a} \subset A$ *is maximal; and suppose*

$$ab \in \mathfrak{a}.$$

Consider the ideal

$$\mathfrak{a}' = \mathfrak{a} + (a) = \{x + ay : x \in \mathfrak{a},\ y in A\}.$$

Evidently

$$\mathfrak{a} \subset \mathfrak{a}' \subset A.$$

Hence, from the maximality of $\mathfrak{a}$*,*

$$\mathfrak{a}' = \mathfrak{a} \text{ or } A.$$

Thus if $a \notin \mathfrak{a}$ *then* $\mathfrak{a}' = A$*. In that case,* $1 \in \mathfrak{a}'$*, ie*

$$x + ay = 1$$

for some $x \in \mathfrak{a},\ y \in A$*. But then, multiplying by* b*,*

$$b = bx + (ab)y,$$

Since $x, ab \in \mathfrak{a}$ *it follows that*

$$b \in \mathfrak{a}.$$

Thus $\mathfrak{a}$ *is prime.*

(d) *No. The ideal* $(0) \subset \mathbb{Z}$ *is prime but not maximal.*

(e) i. *Suppose* A *is a number ring.*

Lemma 6.1. *As an abelian group, A is finitely-generated:*

$$A \cong \mathbb{Z}^r.$$

It follows from this that every ideal $\mathfrak{a} \subset A$ is also finitely-generated as an abelian group.

Lemma 6.2. *Every non-zero ideal $\mathfrak{a} \in A$ contains a non-zero rational integer $n \in \mathbb{Z}$.*

Lemma 6.3. *If $\mathfrak{a} \in A$ is a non-zero ideal then the quotient-ring $A/\mathfrak{a}$ is finite.*

We define the norm of a non-zero ideal $\mathfrak{a} \subset A$ as

$$|\mathfrak{a}| = \#(A/\mathfrak{a}),$$

and set

$$|(0)| = 0.$$

Lemma 6.4. *A finite integral domain is a field.*

Lemma 6.5. *Every non-zero prime ideal $\mathfrak{p} \subset A$ is maximal.*

Lemma 6.6. *Every non-zero ideal $\mathfrak{a} \subset A$ contains a product of maximal ideals:*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}.$$

Proof. We argue by induction on $|\mathfrak{a}|$.
If $\mathfrak{a}$ is prime, the result is immediate.
If not then there exist elements $a, b \in A$ such that

$$ab \in \mathfrak{a}, \quad a, b \notin \mathfrak{a}.$$

Then

$$(\mathfrak{a} + (a))(\mathfrak{a} + (b)) \subset \mathfrak{a}.$$

By the inductive hypothesis,

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a} + (a), \quad \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{a} + (b).$$

Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{a}.$$

□

Suppose A is an integral domain with field of fractions k. A fractional ideal is a non-empty subset $\mathfrak{a} \subset k$ such that $c\mathfrak{a}$ is an ideal in A for some non-zero $c \in k$.

If $\mathfrak{a}$ *is a fractional ideal then we set*

$$\mathfrak{a}^{-1} = \{c \in k : c\mathfrak{a} \subset A\}.$$

It is easy to see that $\mathfrak{a}^{-1}$ *is a fractional ideal, and that*

$$A \subset \mathfrak{a}^{-1}.$$

The non-zero fractional ideal $\mathfrak{a}$ *is said to be invertible if*

$$\mathfrak{a}\mathfrak{a}^{-1} = A.$$

This is the same as saying that there is a fractional ideal $\mathfrak{b}$ *such that*

$$\mathfrak{a}\mathfrak{b} = A.$$

The ideal $\mathfrak{a} \subset A$ *is invertible if and only if there is an ideal* $\mathfrak{b} \subset A$ *such that*

$$\mathfrak{a}\mathfrak{b} = (c),$$

where $c \in A$ *is non-zero.*
If $c \in A,\ c \neq 0$ *and*

$$(c) = \mathfrak{a}_1 \cdots \mathfrak{a}_r$$

then the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *are all invertible.*
We assume again that A *is a number ring.*

Lemma 6.7. *If* $\mathfrak{p} \subset A$ *is maximal then*

$$\mathfrak{p}^{-1} \neq A.$$

Proof. Choose $c \in \mathfrak{p},\ c \neq 0$. Then there exist maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (c).$$

Let us assume that r is minimal.
Since

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (c) \subset \mathfrak{p},$$

one of $\mathfrak{p}_i = \mathfrak{p}$. Let us assume that $\mathfrak{p}_1 = \mathfrak{p}$.
Choose $a \in \mathfrak{p}_2 \cdots p_r,\ a \notin (c)$. Then

$$a\mathfrak{p} \subset (c) \text{ but } a \notin (c).$$

It follows that

$$ac^{-1} \in \mathfrak{p}^{-1} \text{ but } ac^{-1} \notin A.$$

□

Lemma 6.8. *Every maximal ideal $\mathfrak{p} \subset A$ is invertible.*

[This is the main Lemma, and the only one that makes use of the fact that A consists of algebraic integers.]

Proof. Clearly

$$A \subset \mathfrak{p}^{-1},$$

so

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p} \text{ or } A.$$

In the second case $\mathfrak{p}$ is invertible. Suppose then that

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p};$$

and suppose $\alpha \in \mathfrak{p}^{-1}$. Then

$$\alpha\mathfrak{p} \subset \mathfrak{p}.$$

It follows that α is an algebraic integer, ie

$$\alpha \in k \cap \bar{Z} = A.$$

Thus

$$\mathfrak{p}^{-1} \subset A.$$

But we saw earlier that this was not the case; hence $\mathfrak{p}$ is invertible. □

Lemma 6.9. *Every non-zero ideal $\mathfrak{a} \subset A$ is expressible as a product of prime ideals.*

Proof. We argue by induction on $|\mathfrak{a}|$. If $\mathfrak{a}$ is prime there is nothing to prove. Otherwise (from a Lemma above) we can find maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{a}.$$

Let us assume that this is a minimal solution, ie there is no such product with $< r$ maximal ideals.
We know that $\mathfrak{p}_1$ is invertible. Hence

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{p}_1^{-1}\mathfrak{a}.$$

But $\mathfrak{p}_1^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$, since otherwise

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{a},$$

contrary to the minimality of r.
Thus

$$|p_1^{-1}\mathfrak{a}| < |\mathfrak{a}|,$$

and so, by the inductive hypothesis,

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

with $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ maximal.
But then, multiplying by $\mathfrak{p}$,

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

□

Lemma 6.10. *The expression of a non-zero ideal $\mathfrak{a} \subset A$ as a product of maximal ideals is unique up to order.*

Proof. We argue by induction on the minimal number of ideals in such an expression.
Suppose

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Then

$$\mathfrak{q}_1 \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \implies \mathfrak{q}_1 = \mathfrak{p}_i$$

for some i.
We may suppose, after re-ordering the $\mathfrak{p}_i$ if necessary, that $q_1 = \mathfrak{p}_1$. Hence, multiplying by p_1^{-1},

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s,$$

and the result follows by the inductive hypothesis. □

7. Show that the integral

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1}\, dx$$

converges for all $s \in \mathbb{C}$ with $\Re(s) > 0$.

Show how $\Gamma(s)$ can be extended to a meromorphic function in the whole of $\mathbb{C}$, and determine its poles and zeros.

Answer:

(a) *If* $x \in [0, \infty)$ *then*

$$|x^s| = x^\sigma$$

where $\sigma = \Re(s)$. *Since*

$$e^{-x} x^n \to 0 \text{ as } x \to \infty$$

for all n, *the integral converges at the top for all* s.

At the bottom,

$$|x^{s-1}| < x^{-(1+\epsilon)}$$

if $\Re(s) > \epsilon$. *Hence the integral converges at the bottom if* $\Re(s) > 0$.

(b) *If* $\Re(s) > 0$ *then, on integrating by parts,*

$$\begin{aligned}\Gamma(s+1) &= \int_0^\infty e^{-x} x^s \, dx \\ &= \left[-e^{-x} x^s\right]_0^\infty + s \int_0^\infty e^{-x} x^{s-1} \, dx \\ &= s \int_0^\infty e^{-x} x^{s-1} \, dx \\ &= s\, \Gamma(s).\end{aligned}$$

Thus

$$\Gamma(s) = \frac{\Gamma(s+1)}{s}.$$

Now the right-hand side is meromorphic in $\Re(s) > -1$, *with a single simple pole at* $s = 0$; *so this formula defines an analytic continuation of* $\Gamma(s)$ *to* $\Re(s) > -1$.

But repeating this argument, for any integer $r > 0$,

$$\Gamma(s) = \frac{\Gamma(s+r}{s(s+1)\cdots(s+r-1)},$$

defining an analytic continuation of $\Gamma(s)$ *to* $\Re(s) > -r$.

In this way $\Gamma(s)$ *is extended to a meromorphic function in the whole plane* $\mathbb{C}$, *with poles at* $s = 0, -1, -2, \ldots$.

We assume the following result:

Lemma 7.1. *For all* $s \in \mathbb{C} \setminus \mathbb{Z}$,

$$\Gamma(s)\, \Gamma(1-s) = \frac{\pi}{\sin \pi s}.$$

[This identity can be established in various ways. Perhaps the neatest is via the identity

$$\int_0^1 t^{u-1}(1-t)^{v-1}dt = \frac{\Gamma(u)\Gamma(v)}{\Gamma(u+v)},$$

which can be established by expressing $\Gamma(u)\Gamma(v)$ as a double integral.]
It follows from this result that $\Gamma(s)$ has no zeros, since $\sin \pi s$ has no poles.

8. Show that the series

$$\zeta(s) = 1 + 2^{-s} + 3^{-s} + \cdots$$

converges for all $s \in \mathbb{C}$ with $\Re(s) > 1$.

Does it converge for any s with $\Re(s) = 1$?

Show how $\zeta(s)$ can be extended to a meromorphic function in $\Re(s) > 0$.

Answer:

(a) *If $s = \sigma + it$ then*

$$n^s = e^{s \log n} = e^{\sigma \log n}\, e^{it \log n}.$$

Hence

$$|n^s| = e^{\sigma \log n} = n^\sigma.$$

Now

$$\sum n^{-\sigma}$$

converges if $\sigma > 1$, by comparison with

$$\int x^{-\sigma} = \left[\frac{1}{1-\sigma} x^{1-\sigma}\right].$$

[We are using the fact that if $f(x)$ is increasing and > 0 then $\sum f(n)$ and $\int f(x)dx$ converge or diverge together.]
It follows that

$$\sum n^{-s}$$

is absolutely convergent for $\Re(s) > 1$.

(b) The series

$$\sum n^{-s}$$

does not converges for any s on the real line $\Re(s) = 1$.
The result is obvious if $s = 1$, so we may suppose that

$$s = 1 + it,$$

where $t \neq 0$.
We have

$$\begin{aligned} n^{-s} &= \frac{1}{n} n^{-it} \\ &= \frac{1}{n} e^{-it \log n}. \end{aligned}$$

Thus

$$\Re(n^{-s}) = \frac{1}{n} \cos(t \log n);$$

so it is sufficient to show that

$$\sum_n \frac{1}{n} \cos(t \log n)$$

is divergent.
Choose a large integer m, and consider the terms in the interval

$$2m\pi \leq t \log n \leq (2m + 1/4)\pi,$$

ie

$$e^{2m\pi/t} \leq n \leq e^{(2m+1/4)\pi/t} = e^{2m\pi/t}\ e^{\pi/4t}$$

Within this range,

$$\cos(t \log n) \geq \cos \pi/4 = 1/sqrt2,$$

while

$$\frac{1}{n} > e^{-(2m+1/4)\pi/t} = Ce^{-2m\pi/t},$$

where

$$C = e^{-\pi/4t}.$$

The length of the interval is

$$C' e^{2m\pi/t},$$

where

$$C' = e^{\pi/4t} - 1 > 0.$$

Thus the number of integers in the interval is

$$> C' e^{2m\pi/t} - 1.$$

Hence the contribution of these terms — all positive — is

$$\begin{aligned} &> \frac{CC'}{\sqrt{2}} - \frac{C}{\sqrt{2}} e^{-2m\pi/t} \\ &> \frac{CC'}{2} \end{aligned}$$

for sufficiently large M.

We conclude that the series is not convergent.

(c) *We can use Riemann-Stieltjes integration by parts to continue $\zeta(s)$ analytically to $\Re(s) > 0$*

Let

$$f(x) = [x], \quad g(x) = x - [x].$$

Then

$$g(x) = x - f(x),$$

and so

$$\begin{aligned} \sum_1^N n^{-s} &= 1 + \int_1^N x^{-s} df(x) \\ &= 1 + \int_1^N x^{-s} dx - \int_1^N x^{-s} dg(x). \end{aligned}$$

Now

$$\int_1^N x^{-s} dx = \frac{1 - N^{-s+1}}{s-1} \to \frac{1}{s-1} \text{ as } N \to \infty$$

if $\Re(s) > 1$, while

$$\begin{aligned} \int_1^N x^{-s} dg(x) &= \left[x^{-s} g(x)\right]_1^N + s \int_1^N x^{-s-1} g(x) dx \\ &\to 1 + s \int_1^\infty x^{-s-1} g(x) dx \end{aligned}$$

Thus

$$\zeta(s) = \frac{1}{s-1} + s \int_1^\infty x^{-s-1} g(x) dx$$

if $\Re(s) > 1$.

Since $g(x)$ *is bounded, the integral on the right is convergent in* $\Re(s) > 0$*, and defines a holomorphic function there. This formula therefore defines an analytic continuation of* $\zeta(s)$ *to* $\Re(s)$*, as a meromorphic function with a single simple pole at* $s = 1$ *(with residue 1).*

9. Outline the proof of Dirichlet's Theorem, that there are an infinity of primes in any arithmetic sequence $dn + r$ with $\gcd(r, d) = 1$.

Answer:

(a) *Let* χ *be a character of the group* $(\mathbb{Z}/d)^\times$*. We extend* χ *to a function on* $\mathbb{Z}/(d)$ *by setting*

$$\chi(a) = 0 \text{ if } \gcd(a, d) > 1;$$

and we then extend this to a function

$$\chi : \mathbb{Z} \to \mathbb{C}.$$

(b) *We define the corresponding L-function by*

$$L_\chi(s) = \sum_n \frac{\chi(n)}{n^{-s}}.$$

(c) *This series converges absolutely for* $\Re(s) > 1$*, and so defines a holomorphic function there.*

(d) *If* $\chi \neq \chi_0$*, the principal character* mod d *(corresponding to the trivial character of* $(\mathbb{Z}/d)^\times$*) then*

$$\sum_{0 \le n \le d} \chi(n) = 0.$$

[This follows from the orthogonality of the characters.]

(e) *If* $\chi \neq \chi_0$ *then the series converges for* $\Re(s) > 0$*, and so defines a holomorphic function there.*

[This follows from the fact that the partial sums

$$S(x) = \sum_{0 \le n \le x} \chi(n)$$

are bounded. For

$$\begin{aligned} L_\chi(s) &= \int_{1-}^{\infty} x^{-s} dS(x) \\ &= \left[x^{-s} S(x)\right]_{1-}^{\infty} + s \int x^{-s-1} S(x) dx \\ &= s \int x^{-s-1} S(x) dx \end{aligned}$$

and the integral on the right converges for $\Re(s) > 0$, since $S(x)$ is bounded.]

(f) *The L-function can also be analytically continued to $\Re(s) > 0$ if $\chi = \chi_0$, but in this case the function has a simple pole at $s = 1$. [This follows on setting*

$$T(x) = \frac{\phi(d)}{d} x - S(x).$$

For $T(x)$ is bounded, and

$$\begin{aligned} L_{\chi_0}(s) &= \int_{1-}^{\infty} x^{-s} dS(x) \\ &= \int_{1-}^{\infty} x^{-s} (\phi(d/d) dx - \int_{1-}^{\infty} x^{-s} dT(x) \\ &= \frac{\phi(d)}{d} \frac{1}{s-1} + s \int_{1}^{\infty} x^{-s-1} T(x) dx, \end{aligned}$$

on integrating by parts. Since $T(x)$ is bounded, the integral is convergent in $\Re(s) > 0$ and defines a holomorphic function there.]

(g) *$L_\chi(s)$ satisfies the Euler Product Formula*

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

for $\Re(s) > 1$.

(h) *It follows by logarithmic differentiation that*

$$\frac{L'_\chi(s)}{L_\chi(s)} = -\sum_p \log p p^{-s} + h_\chi(s),$$

where $h_\chi(s)$ is holomorphic in $\Re(s) > 1/2$.

(i) *The characters of a finite abelian group G form a basis for the functions on G.*

In particular, we can find a linear combination

$$f(n) = \sum_{\chi} c_\chi \, \chi(n)$$

of the characters of $(\mathbb{Z}/d)^\times$ such that

$$f(n) = \begin{cases} 1 & \text{if } n = r, \\ 0 & \text{if } n \neq r. \end{cases}$$

Since

$$\sum_{0 \le n \le d} \chi(n) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ \phi(d) & \text{if } \chi = chi_0, \end{cases}$$

it follows that

$$c_{\chi_0} = \frac{1}{\phi(d)}.$$

(j) *If now we take the same linear combination of the L-functions we see that*

$$\sum_{\chi} c_\chi \frac{L'_\chi(s)}{L_\chi(s)} = - \sum_{p \equiv r \bmod d} \log p p^{-s} + h(s),$$

where $h(s)$ is holomorphic in $\Re(s) > 1/2$.

10. If there are only a finite number of primes $p \equiv r \bmod d$ then the function on the right is holomorphic in $\Re(s) > 1/2$.

    However, the term on the left corresponding to χ_0 has a simple pole at $s = 1$ since $L_{\chi_0}(s)$ has a pole there.

11. The proof is not quite complete, since if any of the L-functions had a *zero* at $s = 1$ this would contribute a pole on the left, which might cancel out the pole from the χ_0 term.

    Lemma 11.1. $L_\chi(1) \neq 0$ *for any L-function.*

    With this the proof of Dirichlet's Theorem is complete.

    [I gave a proof of the Lemma in the course, but there was a gap in it; it was only valid if χ is non-real.

If χ is real (but $\neq \chi_0$), ie

$$\chi(n) = \pm 1$$

for all n, then a rather complicated calculation shows that

$$L_\chi(1) > 0,$$

and so completes the proof of the Theorem.]