Course 428 — Sample Paper 1

Timothy Murphy

1 Dec 1997

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

1. State carefully, and prove, the Fundamental Theorem of Arithmetic (the Unique Factorisation Theorem) for the natural numbers $\mathbb{N}$.

   Prove that there are an infinity of prime numbers.

   Show that a number $n \equiv 5 \bmod 6$ must have a prime factor $p \equiv 5 \bmod 6$. Hence or otherwise show that there are an infinity of primes $p \equiv 5 \bmod 6$.

   Answer:

   (a) *We say that $p \in \mathbb{N}$ is* prime *if $p > 1$ and*

   $$d \mid p,\ d > 1 \implies d = p.$$

   Theorem 1. *Each natural number $n > 0$ is expressible as a product of prime numbers*

   $$n = p_1 \cdots p_r,$$

   and the expression is unique up to order.

   (b) *The proof of this result depends on Euclid's Lemma*

   Lemma 1. *If p is prime then*

   $$p \mid ab \implies p \mid a \text{ or } p \mid b \quad (a, b \in \mathbb{Z}).$$

   This follows as a bye-product of the euclidean algorithm for computing $d = \gcd(m, n)$ for $m, n \in \mathbb{N}$, which shows that there exist $u, v \in \mathbb{Z}$ such that

   $$um + vn = d.$$

For suppose $p \nmid a$. Then $\gcd(p, a) = 1$, so there exist $u, v \in \mathbb{Z}$ such that

$$up + va = 1.$$

Multiplying by b,

$$upb + vab = b.$$

Since $p \mid ab$ it follows that

$$p \mid b.$$

Lemma 2. *Each integer $n > 1$ is expressible as a product of primes.*

This follows by induction on n. If n is not prime then

$$n = ab,$$

and by induction a, b are expressible as products of primes.

Lemma 3. *The expression for n as a product of primes is unique up to order.*

This also follows by induction on n.
Suppose

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

are two such expressions for n. By Euclid's Lemma,

$$p_1 \mid q_j$$

for some j. Since q_j is prime,

$$p_1 = q_j.$$

The result follows on applying the inductive hypothesis to n/p_1.

(c) *Suppose there are only a finite number of primes, say*

$$p_1, \ldots, p_n.$$

Consider

$$N = p_1 \cdots p_n + 1.$$

Suppose p is a prime factor of N. Then $p = p_i$ for some i, by hypothesis. But

$$p_i \mid N \implies p \mid 1,$$

which is absurd.

(d) *If p is an prime $\neq 2, 3$ then*

$$p \equiv \pm 1 \bmod 6.$$

Suppose

$$n = p_1 \cdots p_r.$$

Then

$$p_1, \ldots, p_r \equiv 1 \bmod 6 \implies n \equiv 1 \bmod 6.$$

So if $n \equiv -1 \bmod 6$ it must have a prime factor $\equiv -1 bmod 6$.

(e) *Suppose there are only a finite number of primes $\equiv -1 \bmod 6$, say*

$$p_1, \ldots, p_n.$$

Consider

$$N = 6p_1 \cdots p_n - 1.$$

Then $N \equiv -1 \bmod 6$; so N has a prime factor $p \equiv -1 \bmod 6$. By hypothesis $p = p_i$ for some i. But as before,

$$p_i \mid N \implies p_i \mid 1,$$

which is absurd.

2. State carefully, and sketch the proof of, Gauss' Law of Quadratic Reciprocity.

   Determine if 173 is a quadratic residue mod297.

   Answer:

   (a)

   Theorem 2. *If p, q are distinct odd primes then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4, \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

   (b) *Here is the proof using permutations that I mentioned in the lectures.*

   Lemma 4. *If p is an odd prime, and $\gcd(a, p) = 1$ then*

$$\left(\frac{a}{p}\right) = \epsilon(\pi),$$

   where $\pi = \pi_a$ is the permutation

$$x \mapsto ax : \mathbb{Z}/(p) \to \mathbb{Z}/(p)$$

   (and $\epsilon(\pi) = \pm 1$ according as π is even or odd).

The proof would not be required in an exam, but I give it here.

Proof. Since $\pi(0) = 0$, we may consider the restriction of π to $(\mathbb{Z}/p)^\times$; this will not affect the parity of the permutation.
Suppose the order of $a \bmod p$ is r. Then the permutation π of $\mathbb{Z}/p)^\times$ consists of $(p-1)/r$ cycles each of length r.
We know that
$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$
Thus π is even if and only if either r is odd or $(p-1)/r$ is even. (Recall that a cycle of odd length is even, while a cycle of even length is odd.)
We know of course that $r \mid p-1$. Thus if r is odd then $r \mid (p-1)/2$ and so $\left(\frac{a}{p}\right) = 1$.
On the other hand if r is even then $r \mid (p-1)/2$ if and only if $(p-1)/r$ is even. □

Alternatively, one could argue as follows:

Proof. There are certainly quadratic non-residues $\bmod p$, since the equivalence
$$a^{(p-1)/2} \equiv 1 \bmod p$$
can be regarded as a polynomial equation
$$x^{(p-1)/2} = 1$$
in the finite field $F_p = \mathbb{Z}/(p)$; and a polynomial equation of degree d over any field has at most d roots.
If we write π_a for the permutation defined by a, then
$$a \longrightarrow \epsilon(\pi_a) : (\mathbb{Z}/p)^\times \longrightarrow \{\pm 1\}$$
is a homomorphism.
In particular
$$a^2 \mapsto 1,$$
ie if $b = a^2$ is a quadratic residue then $\epsilon(\pi_b) = 1$.
Consider the subgroup
$$G = \{a \in (\mathbb{Z}/p)^\times : \epsilon(\pi_a) = 1\}.$$
This contains the subgroup formed by the quadratic residues, which is of index 2. Since G is not the whole group, it must be this subgroup. □

That is just the hors d'oevre. Now for the main part of the proof.
By the Chinese Remainder Theorem, the map

$$\gamma : a \bmod pq \mapsto (a \bmod p, a \bmod q) : \mathbb{Z}/(pq) \to \mathbb{Z}/(p) \times \mathbb{Z}/(q)$$

is an isomorphism.
We consider two maps in the opposite direction,

$$\alpha, \beta : \mathbb{Z}/(p) \times \mathbb{Z}/(q) \to \mathbb{Z}/(pq),$$

given by

$$\alpha(a, b) = a + pb, \quad \beta(a, b) = qa + b \qquad (0 \le a < p, 0 \le b < q).$$

If we imagine $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ *as a* $p \times q$ *array of numbers then we can think of* α *as the ordering of the* pq *entries by column, and* β *as the ordering by rows.*
Since

$$\gamma\alpha(a, b) = (a, qb),$$

$\gamma\alpha$ *permutes each row of the array by the permutation* π_q*. Thus*

$$\begin{aligned} \epsilon(\gamma\alpha) &= \epsilon(\pi_q)^p \\ &= \epsilon(\pi_q) \\ &= \left(\frac{q}{p}\right). \end{aligned}$$

Similarly,

$$\epsilon(\gamma\beta) = \left(\frac{p}{q}\right).$$

The permutation

$$\alpha\beta^{-1} : \mathbb{Z}/(pq) \to \mathbb{Z}/(pq)$$

can be written

$$qa + b \mapsto a + pb \qquad (0 \le a < p,\ 0 \le b < q).$$

Recall that if π *is a permutatation of* $1, \ldots, n$ *then*

$$\epsilon(\pi) = (-1)^{\mu},$$

where μ *is the number of reversals of order under* π*, ie the number of pairs* (i, j) *with* $1 \leq i < j \leq n$ *such that*

$$\pi(i) > \pi(j).$$

So $\epsilon(\alpha\beta^{-1}) = (-1)^\mu$*, where* μ *is the number of pairs (of pairs)*

$$(a, b),\ (a', b')$$

with

$$qa + b < qa' + b',$$

ie

$$a < a' \text{ or } a = a'\ b < b'$$

such that

$$a + pb > a' + pb',$$

ie

$$b > b' \text{ or } b = b'\ a > a'.$$

Clearly there will be no reversal of order if $a = a'$*, so we need only consider the cases where* $a < a'$*. Again, there cannot be a reversal of order if* $b = b'$*. So* μ *is the number of cases with*

$$a < a' \text{ and } b > b'.$$

These are independent conditions; and the total number of solutions is

$$\frac{p(p-1)}{2}\ \frac{q(q-1)}{2}.$$

Thus

$$\begin{aligned}(-1)^\mu &= (-1)^{\frac{p(p-1)}{2}}\ (-1)^{\frac{q(q-1)}{2}}\\ &= (-1)^{\frac{(p-1)}{2}}\ (-1)^{\frac{(q-1)}{2}},\end{aligned}$$

since p, q *are odd.*
Hence

$$\epsilon(\alpha\beta^{-1}) = (-1)^{\frac{p-1}{2}\ \frac{q-1}{2}},$$

while

$$\epsilon(\gamma\alpha) = \left(\frac{q}{p}\right), \quad \epsilon(\gamma\beta) = \left(\frac{p}{q}\right).$$

Since

$$(\gamma\beta)^{-1}(\gamma\alpha) = \beta^{-1}\alpha,$$

it follows that

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

But

$$\epsilon(\beta^{-1}\alpha) = \epsilon(\alpha\beta^{-1});$$

for

$$\alpha\beta^{-1} = \beta(\beta^{-1}\alpha)\beta^{-1},$$

and if $f : X \to Y$ *is a bijection between finite sets, and* π *is a permutation of* X *then* $f\pi f^{-1}$ *is a permutation of* Y*, and*

$$\epsilon(f\pi f^{-1}) = \epsilon(\pi).$$

We conclude that

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

which is what we had to prove.

(c) *Here is a third proof, using Gauss sums. This is by far the best proof - since the method has many applications in other areas - except that it has one surprising point of difficulty.*
Let

$$\epsilon(x) = e^{2\pi i x}.$$

We define the Gauss sum

$$E(a, n) = \sum_{0 \le j < n} \epsilon\left(\frac{ax^2}{p}\right).$$

Lemma 5. *If* p *is an odd prime, and* $p \nmid a$,

$$E(a, p) = \left(\frac{a}{p}\right) E(1, p).$$

Proof. Suppose

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

say

$$a \equiv b^2 \bmod p.$$

Then

$$\begin{aligned} E(a,p) &= \sum \epsilon\left(\frac{ax^2}{p}\right) \\ &= \sum \epsilon\left(\frac{(bx)^2}{p}\right) \\ &= \sum \epsilon\left(\frac{x^2}{p}\right) \\ &= E(1,p), \end{aligned}$$

since bx runs over a complete set of residues mod p as x does.

Now suppose

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

As x runs over a set of residues mod p coprime to p, ax^2 runs over the quadratic non-residues mod p, each one twice. Hence

$$\begin{aligned} E(a,p) + E(1,p) &= 2\sum \epsilon\left(\frac{x}{p}\right) \\ &= 0. \end{aligned}$$

Hence

$$\begin{aligned} E(a,p) &= -E(1,p) \\ &= \left(\frac{a}{p}\right) E(1,p). \end{aligned}$$

□

Lemma 6. *If p, q are distinct odd primes then*

$$E(p,q)E(q,p) = E(1,pq).$$

Proof. We have

$$\begin{aligned}
E(p,q)E(q,p) &= \sum_{0 \le x < q} \epsilon\left(\frac{px^2}{q}\right) \sum_{0 \le x < p} \epsilon\left(\frac{qy^2}{p}\right) \\
&= \sum_{0 \le x < q,\, 0 \le x < p} \epsilon\left(\frac{p^2x^2 + q^2y^2}{pq}\right) \\
&= \sum_{0 \le x < q,\, 0 \le y < p} \epsilon\left(\frac{(px+qy)^2}{pq}\right) \\
&= \sum_{0 \le z < pq} \epsilon\left(\frac{z^2}{pq}\right) \\
&= E(1,pq),
\end{aligned}$$

since $px + qy$ runs over the residues mod pq by the Chinese Remainder Theorem. □

Evidently the complex conjugate

$$\begin{aligned}
\overline{E(a,n)} &= \sum \epsilon\left(\frac{-ax^2}{n}\right) \\
&= E(-a,n).
\end{aligned}$$

In particular, if p is an odd prime and $p \nmid a$ then

$$\begin{aligned}
\overline{E(a,p)} &= E(-a,p) \\
&= \left(\frac{-1}{p}\right) E(a,p).
\end{aligned}$$

It follows that

$$E(a,p) \begin{cases} \in \mathbb{R} \ \textit{if } p \equiv 1 \bmod 4 \\ \in i\mathbb{R} \ \textit{if } p \equiv 3 \bmod 4. \end{cases}$$

Lemma 7. *If p is an odd prime then*

$$|E(1,p)| = \sqrt{p}.$$

Proof. We have

$$\begin{aligned}
|E(1,p)|^2 &= E(1,p)\ \overline{E(1,p)} \\
&= \sum_{0 \le x,y < p} \epsilon\left(\frac{x^2 - y^2}{p}\right).
\end{aligned}$$

Suppose $p \nmid a$. Then

$$x^2 - y^2 \equiv a \bmod p$$

has just $p-1$ solutions, given by

$$x - y = t,\ x + y = a/t$$

for $t = 1, 2, \ldots, p-1$.
On the other hand

$$x^2 - y^2 \equiv 0 \bmod p$$

has $2p-1$ solutions $(0,0), (1, \pm 1), \ldots, (p-1, \pm(p-1))$.
Thus

$$\begin{aligned}\sum_{0 \le x,y < p} \epsilon\left(\frac{x^2 - y^2}{p}\right) &= (2p-1) + (p-1) \sum_{1 \le a \le p-1} \epsilon\left(\frac{a}{p}\right) \\ &= (2p-1) + (p-1)(-1) \\ &= p.\end{aligned}$$

Hence

$$|E(1,p)|^2 = p.$$

□

It follows that

$$E(1,p) = \begin{cases} \pm\sqrt{p} \text{ if } p \equiv 1 \bmod 4 \\ \pm i\sqrt{p} \text{ if } p \equiv 3 \bmod 4 \end{cases}$$

In fact the positive sign holds in each case:

$$E(1,p) = \begin{cases} \sqrt{p} \text{ if } p \equiv 1 \bmod 4 \\ \sqrt{p} \text{ if } p \equiv 3 \bmod 4 \end{cases}$$

It is this that is surprisingly difficult to establish.

(d) *While 173 is prime,*

$$297 = 3^3 \cdot 11.$$

Since

$$\left(\frac{173}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

173 is not a quadratic residue mod3. *So* a fortiori *it is not a quadratic residue* mod297

3. Define an *algebraic number* and an *algebraic integer*. Show that the algebraic numbers form a field $\bar{\mathbb{Q}}$, and that the algebraic integers form a ring $\bar{\mathbb{Z}}$.

Prove that
$$\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Show that every algebraic number α is expressible in the form
$$\alpha = \frac{\beta}{n}$$
where β is an algebraic integer, and $n \in \mathbb{N}$.

Answer:

(a) *We say that $\alpha \in \mathbb{C}$ is an* algebraic number *if it satisfies an equation of the form*
$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$
with $a_1, \ldots, a_n \in \mathbb{Q}$.

(b) *We say that α is an* algebraic integer *if it satisfies an equation of the form*
$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$
with $a_1, \ldots, a_n \in \mathbb{Z}$.

(c) *We have to show that if $\alpha, \beta \in \bar{\mathbb{Q}}$ then $\alpha + \beta,\ \alpha\beta \in \bar{\mathbb{Q}}$; and if $\alpha \neq 0$ then $\alpha^{-1} \in \bar{\mathbb{Q}}$.*

Suppose α, β satisfy the equations
$$f(x) = x^m + a_1 x^{m-1} + \cdots a_m,$$
$$g(x) = x^n + b_1 x^{n-1} + \cdots b_n,$$
where $a_i, b_j \in \mathbb{Q}$.

If $\alpha = 0$ or $\beta = 0$ the result is obvious; so we may suppose that $a_m.b_n \neq 0$.

Let the roots of these equations be $\alpha = \alpha_1, \ldots, \alpha_m$ and $\beta = \beta_1, \ldots, \beta_n$, so that
$$f(x) = (x - \alpha_1) \cdots (x - \alpha_m),$$
$$g(x) = (x - \beta_1) \cdots (x - \beta_n).$$

Let

$$s(x) = \prod_{i,j}(x - \alpha_i - \beta_j),$$
$$p(x) = \prod_{i,j}(x - \alpha_i\beta_j).$$

Then

$$s(x) = \prod_i g(x - \alpha_i).$$

The coefficients of $s(x)$ are symmetric polynomials in the α_i. It follows from the theory of symmetric polynomials that they are expressible as polynomials in the coefficients of $f(x)$, and so are in $\mathbb{Q}$. Thus $s(x) \in \mathbb{Q}[x]$, and so

$$\alpha + \beta \in \bar{\mathbb{Q}}.$$

Similarly

$$\begin{aligned} p(x) &= (\prod_i \alpha_i)^n \prod_{i,j}(x/\alpha_i - \beta_j) \\ &= (\prod_i \alpha_i)^n \prod_i g(x/\alpha_i) \\ &= \prod_i g_i(x), \end{aligned}$$

where

$$g_i(x) = x^n + a_1\alpha_i + \cdots + a_n\alpha_i^n.$$

Again, the coefficients of $p(x)$ are symmetric polynomials in the α_i, and so are in $\mathbb{Q}$. Thus

$$\alpha\beta \in \bar{\mathbb{Q}}.$$

Finally, α^{-1} satisfies the equation

$$a_m + a_{m-1}x + \cdots + a_1x^{m-1} + 1 = 0.$$

Hence

$$\alpha^{-1} \in \bar{\mathbb{Q}}.$$

(d) *If*

$$\alpha, \beta \in \bar{\mathbb{Z}},$$

then we may assume that the coefficients $a_i, b_j \in \mathbb{Z}$.

In this case the coefficients of $s(x), p(x)$ *are symmetric polynomials in the* α_i *with integer coefficients; and the theory of symmetric polynomials shows that they are expressible as polynomials in the coefficients* a_i *with integer coefficients. Hence the coefficients of* $s(x), p(x)$ *are in* $\mathbb{Z}$, *and so*

$$\alpha, \beta \in \bar{\mathbb{Z}}.$$

(e) *Suppose* $\alpha \in \bar{\mathbb{Z}}$, *say* α *satisfies*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

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

Now suppose $\alpha \in \mathbb{Q}$, *say*

$$\alpha = \frac{u}{v},$$

where $u, v \in \mathbb{Z}$ *with* $\gcd(u, v) = 1$. *Then*

$$u^n + a_1 u^{n-1} v + \cdots + a_n v^n = 0.$$

It follows that

$$v \mid u^n.$$

Since $\gcd(u, v) = 1$, *this implies that* $v = \pm 1$, *ie*

$$\alpha \in \mathbb{Z}.$$

(f) *Suppose* $\alpha \in \bar{\mathbb{Q}}$, *say* α *satisfies*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

with $a_i \in \mathbb{Q}$.

Multiplying by the lcm of the denominators of the a_i, *we can write this as*

$$b_0 x^n + b_1 x^{n-1} + \cdots + b_n = 0,$$

with $b_i \in \mathbb{Z}$. *But now*

$$(b_0 x)^n + b_0 b_1 (b_0 x)^{n-1} + \cdots + b_0^n b_n = 0,$$

and so

$$\beta = b_0\alpha$$

satisfies the equation

$$x^n + b_0 b_1 x^{n-1} + \cdots + b_0^n b_n = 0.$$

Thus $\beta \in \bar{\mathbb{Z}}$, *and*

$$\alpha = \frac{\beta}{b_0},$$

with $b_0 \in \mathbb{Z}$.

4. State carefully, and prove, the Fundamental Theorem of Arithmetic in the ring $\mathbb{Z}[i]$ of gaussian integers.

   Show that the prime number $p \in \mathbb{N}$ remains prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \bmod 4$.

   Determine the number of ways of expressing 1075 as a sum of 2 squares (of natural numbers).

   Answer:

   (a) *We say that*

   $$\pi \in \Gamma = \mathbb{Z}[i]$$

   is a prime *if*

   $$\pi = \alpha\beta \implies \alpha \text{ or } \beta \text{ is a unit} \qquad (\alpha, \beta \in \Gamma).$$

   (We say that $\epsilon \in \Gamma$ *is a* unit *if it is invertible in* Γ*.)*

   Theorem 3. *Each non-unit* $\alpha \in \Gamma$ *is expressible as a product of primes,*

   $$\alpha = \pi_1 \cdots \pi_r;$$

   and the expression is unique up to order, ie if

   $$\alpha = \pi'_1 \cdots \pi'_{r'}$$

   is a second such expression, then $r' = r$ *and there is a permutation* σ *of* $\{1, \ldots, r\}$ *such that, for each* i,

   $$\pi'_{\sigma(i)} = \epsilon_i \pi_i,$$

   where ϵ_i *is a unit.*

(b) For
$$\gamma = x + yi \in \mathbb{Q}[i]$$
we set
$$|\gamma| = \gamma\,\bar{\gamma} = x^2 + y^2.$$
Evidently,
$$|\gamma_1\gamma_2| = |\gamma_1|\,|\gamma_2|.$$
Lemma 8. *If* $\alpha \in \Gamma$ *then*
$$\alpha \textit{ is a unit } \iff |\gamma| = 1.$$
Lemma 9. *Given*
$$\gamma = x + yi \in \mathbb{Q}[i]$$
we can find $\alpha \in \Gamma$ *such that*
$$|\gamma - \alpha| \leq \frac{1}{2}.$$
Corollary 1. *Given* $\alpha, \beta \in \Gamma$ *(with* $\beta \neq 0$*) there exists* $\gamma, \delta \in \Gamma$ *such that*
$$\alpha = \gamma\beta + \delta,$$
with
$$|\delta| < |\beta|.$$
This allows us to set up the Euclidean Algorithm, from which we derive the following result.

Lemma 10. *Given* $\alpha, \beta \in \Gamma$ *there exists*
$$\delta = \gcd(\alpha, \beta)$$
such that $\delta \mid \alpha\beta$ *and*
$$\delta' \mid \alpha\beta \implies \delta' \mid \delta.$$
Furthermore there exist $u, vin\Gamma$ *such that*
$$u\alpha + v\beta = \delta.$$
Corollary 2. *If* π *is prime that*
$$\pi \mid \alpha\beta \implies \pi \mid \alpha \textit{ or } \pi \mid \beta.$$
Lemma 11. *Each* $\alpha \in \Gamma$ *is expressible as a product of primes.*

This follows by induction on $|\alpha|$.

Lemma 12. *The expression is unique up to order.*

This follows again by induction on $|\alpha|$.
For if we have two expressions, as above, then

$$\pi_1 \mid \pi'_j$$

for some j, and so (since π'_j is prime)

$$\pi'_j = \epsilon\pi_1$$

for some unit ϵ.
The result follows on applying the inductive hypothesis to α/π_1.

(c) *Let p be a rational prime.*

i. *Suppose*

$$p \equiv 3 \bmod 4;$$

and suppose p is not prime in Γ, say

$$p = \alpha\beta.$$

Then

$$|p| = p^2 = |\alpha|\ |\beta|.$$

It follows that

$$|\alpha| = |\beta| = p.$$

Thus if $\alpha = u + vi$ then

$$a^2 + b^2 = p.$$

Hence

$$a^2 + b^2 \equiv 3 \bmod 4,$$

which is impossible.

ii. *Suppose*

$$p \equiv 1 \bmod 4;$$

We know that

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

It follows that

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

ie there exists a such that

$$a^2 + 1 \equiv 0 \bmod p.$$

Thus

$$p \mid (a+i)(a-i).$$

If p were prime in Γ *then this would imply that*

$$p \mid a \pm i,$$

which is absurd.

iii. Since

$$2 = (1+i)(1-i),$$

2 is not prime in Γ

We conclude that p remains prime in Γ *if and only if* $p \equiv 3 \bmod 4$.

(d) We have

$$1075 = 5^2 \cdot 43.$$

Suppose

$$1075 = a^2 + b^2 = (a+bi)(a-bi).$$

We know that 43 is prime in Γ. *Hence*

$$43 \mid a \pm bi,$$

ie

$$43 \mid a, b.$$

But then 43 divides both factors, and so

$$43^2 \mid 1075,$$

which is not true.

Hence 1075 cannot be expressed as the sum of two squares.

5. Prove that if $m > 0$ is not a square then Pell's equation

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

has an infinity of solutions.

Does the equation

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

have a solution in the cases $m = 3, 5, 7$?

Answer:

(a)

Lemma 13. *If $\alpha \in \mathbb{R}$ there are an infinity of integers p, q with*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}.$$

Applying this with $\alpha = \sqrt{m}$, there are an infinity of p, q with

$$|\sqrt{m} - \frac{p}{q}| < \frac{1}{q^2}.$$

But then

$$|\sqrt{m} + \frac{p}{q}| < 2\sqrt{m} + 1,$$

and so

$$|m - \frac{p^2}{q^2}| < \frac{N}{q^2},$$

where $N = [2\sqrt{m}] + 1$.
Thus there are an infinity of integers x, y such that

$$|x^2 - my^2| < N.$$

Consider the remainders $x, y \bmod N$. There must be some integers $a, b \in [0, N)$ such that there are an infinity of solutions with

$$x \equiv a, \ y \equiv b \mod N.$$

Let $(x, y), (X, Y)$ be two such solutions, ie

$$x \equiv X \equiv a, \quad x \equiv X \equiv a, \quad bmodN.$$

Now

$$(x^2 - my^2)(X^2 - mY^2) = (xX - myY)^2 - m(xY - yX)^2.$$

But modulo N,

$$\begin{aligned} xX - myY &\equiv x^2 - my^2 = N \\ &\equiv 0, \end{aligned}$$

while

$$\begin{aligned} xY - yX &\equiv xy - yx \\ &\equiv 0. \end{aligned}$$

Thus

$$N \mid xX - myY,\ xY - yX;$$

and so if we set

$$u = \frac{xX - myY}{N},\ v = \frac{xY - yX}{N}$$

then

$$u^2 - mv^2 = 1.$$

(b) i. *The equation*

$$x^2 - 3y^2 = -1$$

has no integer solution. For one of x, y *must be even, and one odd. But*

$$u^2 \equiv 0 \text{ } or \text{ } 1 \bmod 4.$$

It follows that

$$x^2 - 3y^2 \equiv 0, 1 or 2 \bmod 4.$$

ii. *The equation*

$$x^2 - 5y^2 = -1$$

has the solution $x = 2,\ y = 1$.

iii. *The equation*

$$x^2 - 7y^2 = -1$$

has no integer solution. For

$$u^2 \equiv 0, 1 \text{ } or \text{ } 4 \bmod 8,$$

and so

$$x^2 - 7y^2 \equiv x^2 + y^2 \equiv 0, 1, 2, 4 or \text{ } 5 \bmod 8.$$

6. Express $\sqrt{7}$ as a continued fraction.

   Show that if the continued fraction for a number $\alpha \in \mathbb{R}$ is periodic then α is a quadratic surd.

   Sketch the proof of the converse, that any quadratic surd has a periodic continued fraction.

   Answer:

(a) We have

$$\sqrt{7} = 2 + (\sqrt{7} - 2);$$

and

$$\begin{aligned}\frac{1}{\sqrt{7}-2} &= \frac{\sqrt{7}+2}{3} \\ &= 1 + \frac{\sqrt{7}-1}{3}.\end{aligned}$$

Now

$$\begin{aligned}\frac{3}{\sqrt{7}-1} &= 3\ \frac{\sqrt{7}+1}{6} \\ &= 1 + \frac{\sqrt{7}-1}{2};\end{aligned}$$

and

$$\begin{aligned}\frac{2}{\sqrt{7}-1} &= 2\ \frac{\sqrt{7}+1}{6} \\ &= 1 + \frac{\sqrt{7}-2}{3}.\end{aligned}$$

We are back to where we started; so

$$\sqrt{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}$$

(b) Suppose the continued fraction for α is periodic, say

$$\alpha = [a_0, \dots, a_r, \dot{b_1}, dots, \dot{b_s}]$$

Then

$$\begin{aligned}\alpha &= [a_0, \dots, a_r, \beta] \\ &= \frac{p_r + p_{r-1}\beta}{q_r + q_{r-1}\beta},\end{aligned}$$

where

$$\beta = [\dot{b_1}, \dots, \dot{b_s}]$$

and p_i/q_i is the ith convergent to α.

If we show that β is a quadratic surd it will follow that α is a quadratic surd.
But

$$\begin{aligned}\beta &= [\dot{b}_1, \ldots, \dot{b}_s] \\ &= \frac{p'_s + p'_{s-1}\beta}{q'_s + q'_{s-1}\beta},\end{aligned}$$

where p'_i/q'_i is the ith convergent to β.
Thus β satisfies the quadratic equation

$$q'_{s-1}x^2 + (q'_s - p'_{s-1})x - p_s = 0,$$

and so is a quadratic surd.

(c) *Suppose*

$$\alpha = [a_0, a_1, \cdots]$$

is a quadratic surd, say α satisfies

$$Q(x) = Ax^2 + 2Bx + C = 0,$$

where $A, B, C \in \mathbb{Z}$.
Let

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

Then

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}.$$

Hence

$$A(p_{n-1}\alpha_n + p_{n-2})^2 + 2B(p_{n-1}\alpha_n + p_{n-2})(q_{n-1}\alpha_n + q_{n-2}) + C(q_{n-1}\alpha_n + q_{n-2})^2 = 0.$$

ie

$$A_n\alpha_n^2 + B_n\alpha_n + C_n,$$

with

$$\begin{aligned}A_n &= Ap_{n-1}^2 + 2Bp_{n-1}q_{n-1} + Cq_{n-1}^2 \\ &= q_{n-1}^2\, Q(p_{n-1}/q_{n-1}), \\ B_n &= Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + Cq_{n-1}q_{n-2} \\ &= q_{n-1}q_{n-2}\, Q_1(p_{n-1}/q_{n-1}, p_{n-2}/q_{n-2}), \\ C_n &= Ap_{n-2}^2 + 2Bp_{n-2}q_{n-2} + Cq_{n-2}^2 \\ &= q_{n-2}^2\, Q(p_{n-2}/q_{n-2}),\end{aligned}$$

where

$$Q_1(x,y) = Axy + B(x+y) + C$$

is the 'polarized' form of the quadratic form $Q(x)$.
We shall show that A_n, B_n, C_n do not get large; this follows from the fact that p_i/q_i is very close to α. More precisely,

$$|\alpha - \frac{p_i}{q_i}| \le \frac{1}{q_i q_{i+1}} \le \frac{1}{q_i^2}$$

[since α lies between p_i/q_i and p_{i+1}/q_{i+1} and $p_i q_{i+1} - q_i p_{i+1} = \pm 1$].
Now

$$Q(x) - Q(y) = (x-y)(A(x+y)+B).$$

Hence

$$\begin{aligned} Q(p_i/q_i) &= Q(p_i/q_i) - Q(\alpha) \\ &= (p_i/q_i - \alpha)(A(\alpha + p_i/q_i) + B), \end{aligned}$$

and so

$$\begin{aligned} |Q(p_i/q_i)| &\le |\alpha - p_i/q_i|\ |A|(2|\alpha|+1) + |B|, \\ &\le C\ \frac{1}{q_i^2}, \end{aligned}$$

where $C = 2(|\alpha|+1) + |B|$. Thus

$$|A_n| \le C, \quad |C_n| \le C.$$

Finally,

$$\begin{aligned} Q_1(x,y) - Q_1(x',y') &= A(xy - x'y') + B(x - x' + y - y') \\ &= (x-x')(Ay+B) + (y-y')(Ax'+B). \end{aligned}$$

Thus

$$\begin{aligned} Q_1(p_{n-1}/q_{n-1}, p_{n-2}/q_{n-2}) &= Q_1(p_{n-1}/q_{n-1}, (p_{n-2}/q_{n-2}) - Q_1(\alpha,\alpha) \\ &= (p_{n-1}/q_{n-1} - \alpha)(Ap_{n-1}/q_{n-1} + B) + (p_{n-2}/q_{n-2} - \alpha)(A\alpha \end{aligned}$$

and so

$$\begin{aligned} |Q_1(p_{n-1}/q_{n-1}, p_{n-2}/q_{n-2})| &\le C\ (|\alpha - p_{n-1}/q_{n-1}| + |\alpha - p_{n-2}/q_{n-2}|) \\ &\le C\ \left(\frac{1}{q_{n-1}q_n} + \frac{1}{q_{n-2}q_{n-1}}\right). \end{aligned}$$

Thus

$$absB_n \leq 2C.$$

It follows that the α_n *are roots of a finite number of quadratics; and so there must be a repetition,*

$$\alpha_{m+r} = \alpha_m.$$

In other words, the continued fraction for α *is periodic.*

7. Express 2/3 as a 2-adic number in standard form

$$a_0 + a_1 2 + a_2 2^2 + \cdots \quad (a_i \in \{0, 1\}).$$

Show that the equation

$$x^2 - 7 = 0$$

has no solution in the 2-adic ring $\mathbb{Z}_2$, while the equation

$$x^2 + 7 = 0$$

has just two solutions.

Answer:

(a) *We have*

$$\frac{2}{3} \equiv 0 \bmod 2,$$

and

$$\frac{1}{2}\frac{2}{3} = \frac{1}{3}.$$

Next

$$\frac{1}{3} \equiv 1 \bmod 2,$$

and

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

Continuing

$$\frac{-1}{3} \equiv 1 \bmod 2,$$

and

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

Again,

$$\frac{-2}{3}\equiv 0 \bmod 2,$$

and

$$\frac{1}{2}\,\frac{-2}{3})=\frac{-1}{3}.$$

We are back to where we were 2 steps ago. Thus

$$\frac{2}{3}=0\cdot 1+1\cdot 2+1\cdot 2^2+0\cdot 2^3+1\cdot 2^4+0\cdot 2^5+\cdots,$$

ie

$$\frac{2}{3}=2+2^2+2^4+2^6+\cdots.$$

Checking,

$$\begin{aligned}2+2^2+2^4+2^6+\cdots&=2+\frac{2^2}{1-2^2}\\&=2-\frac{4}{3}\\&=\frac{2}{3}.\end{aligned}$$

*[**Remark**. One could work in the opposite direction, by computing the order of 2* mod3 *(in this case). Thus*

$$2^2\equiv 1 \bmod 3,$$

ie

$$3\mid(1-2^2)$$

In fact

$$\frac{1}{1-2^2}=\frac{-1}{3},$$

and so

$$\begin{aligned}\frac{2}{3} &= 1 + \frac{-1}{3} \\ &= 1 + \frac{1}{1-2^2},\end{aligned}$$

as we saw.

Let us look at a slightly more complicated example from this point of view: Suppose we are asked to express $2/5$ *as a 3-adic integer. The order of* $3 \bmod 5$ *is 4:*

$$3^4 - 1 = 80 = 5 \cdot 16.$$

Thus

$$\frac{1}{5} = \frac{-16}{1-3^4},$$

and so

$$\begin{aligned}\frac{2}{5} &= \frac{-32}{1-3^4} \\ &= 1 + \frac{81-32}{1-3^4} \\ &= 1 + \frac{49}{1-3^4}\end{aligned}$$

Now express 49 in the usual way to base 3:

$$49 = 3^3 + 2 \cdot 2^3 + 3 + 1.$$

Thus

$$\begin{aligned}\frac{2}{5} &= (1 + 3 + 2 \cdot 3^2 + 3^3)(1 + 3^4 + 3^8 + \cdots) \\ &= 1 + 3 + 2 \cdot 3^2 + 3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + \cdots .]\end{aligned}$$

(b) *The congruence*

$$x^2 - 7 \equiv 0 \bmod 2^2$$

has no solution, since

$$x^2 \equiv 0 \text{ or } 1 \bmod 4.$$

Hence

$$x^2 - 7 = 0$$

has no solution in $\mathbb{Z}_2$.
[If

$$x = a_0 + a_1 2 + a_2 2^2 + \cdots$$

were a solution in $\mathbb{Z}_2$, then

$$x = a_0 + a_1 2$$

would be a solution of the congruence

$$x^2 - 7 \equiv 0 \bmod 2^2.]$$

(c) $\mathbb{Z}_2$ is an integral domain. Hence if $\theta \in \mathbb{Z}_2$ were a solution of

$$x^2 + 7 = 0$$

then

$$x^2 + 7 = (x - \theta)(x + \theta),$$

and so there would be just two solutions, $\pm\theta$.
To see that there is a solution, we start with the solution $x = 1$ to the congruence

$$x^2 + 7 \equiv 0 \bmod 2^3.$$

We must show that we can extend this to a solution $\bmod 2^e$ for all e.
Suppose

$$x^2 + 7 \equiv 0 \bmod 2^e,$$

where $e \geq 3$. We want to extend this to a solution $\bmod 2^{e+1}$.
If this solution already satisfies

$$x^2 + 7 \equiv 0 \bmod 2^{e+1}$$

then there is nothing to do. Otherwise

$$x^2 + 7 \equiv 2^e \bmod 2^{e+1}.$$

In this case,

$$\begin{aligned}(x^2 + 2^{e-1})^2 + 7 &\equiv x^2 + 2 \cdot 2^e x + 7 \bmod 2^{e+1}\\ &\equiv 2^e + 2^e \bmod 2^{e+1}\\ &\equiv 0 \bmod 2^{e+1}.\end{aligned}$$

Thus $x + 2^{e-1}$ is a solution $\bmod 2^{e+1}$.
In this way we can extend the solution indefinitely, to give a solution in $\mathbb{Z}_2$.
Remarks

i. *The argument could be expressed very simply in this case, because there are only 2 congruence classes* mod2*. But a similar argument works for an odd prime p as well. The essential point is that if we have a solution* $x \bmod p^e$ *of a polynomial equation* $f(x) = 0$ *(where* $f(x) \in \mathbb{Z}[x]$*) then*

$$f(x + zp^e) \equiv 0 \bmod p^{e+1}$$

reduces to a linear equation for $z \bmod p$*, ie the solution of a linear equation in the field* $\mathbb{F}_p = \mathbb{Z}/(p)$*.*
That is the essential content of Hensel's Lemma, which states that: if x *is a solution of*

$$f(x) \equiv 0 \bmod p^e$$

and

$$f'(x) \not\equiv 0 \bmod p$$

then x *can be extended uniquely to a solution* $\bmod p^{e+1}$.

ii. *There is a completely different way of solving this, using a bit of 'p-adic analysis'.*
By the binomial theorem,

$$\begin{aligned}\sqrt{-7} &= (1 - 2^3)^{1/2} \\ &= 1 - (1/2)2^3 + \frac{1/2 \cdot -1/2}{1 \cdot 2} 2^6 + \frac{1/2 \cdot -1/2 \cdot -3/2}{1 \cdot 2 \cdot 3} 2^9 + \cdots .\end{aligned}$$

We need only ensure that the power of 2 in 2^{3n} *more than swamps the power of 2 in the binomial coefficient*

$$\binom{1/2}{n}.$$

The power of 2 in the numerator of this is 2^{-n}*; while if*

$$2^e || n!$$

then

$$\begin{aligned}e &= \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \cdots \\ &\le \frac{n}{2} + \frac{n}{2^2} + \cdots \\ &\le n.\end{aligned}$$

Hence

$$\binom{1/2}{n} 2^{3n} \equiv 0 \bmod 2^n,$$

and the binomial series converges.
(Recall that

$$\sum a_n$$

converges in $\mathbb{Z}_p$ *if and only if*

$$a_n \to 0.)$$

Note that the solution to

$$x^2 + 7 = 0$$

obtained in this way is not in standard format; but there is nothing wrong with that.

8. Show that a Dirichlet series

$$a_1 + a_2 2^{-s} + a_3 3^{-s} + \cdots \quad (a_i \in \mathbb{C})$$

converges in some half-plane $\Re(s) > \sigma$, and diverges in $\Re(s) < \sigma$.

Show that $\sigma = 1$ for the Riemann zeta function $\zeta(s)$

Show how the definition of $\zeta(s)$ can be extended to $\Re(s) > 0$ by considering the function $(1 - 2^{1-s})\zeta(s)$, and deduce that $\zeta(s)$ has just one pole in this region.

Could this technique be used to extend the definition of $\zeta(s)$ to the whole complex plane?

Answer:

(a)

Lemma 14. *The series*

$$\sum b_n c_n$$

converges if

i. The partial sums

$$B_n = \sum_{r \le N} b_r$$

are bounded; and

ii.
$$\sum |c_n - c_{n+1}|$$
is convergent.

Let
$$f(s) = a_1 + a_2 2^{-s} + a_3 3^{-s} + \cdots .$$
We have to show that if $f(s)$ is convergent for $s = s_0$ then it is convergent for all s with
$$\Re(s) > \Re(s_0).$$

Let
$$s = s_0 + s',$$
where
$$\sigma' = \Re(s') > 0.$$
On applying the Lemma with
$$b_n = a_n n^{-s_0},\ c_n = n^{-s'}$$
the result will follow if we show that
$$\sum |n^{-s'} - (n+1)^{-s'}|$$
is convergent.

Now
$$\begin{aligned} n^{-s'} - (n+1)^{-s'} &= \left[-x^{-s'} \right]_n^{n+1} \\ &= s' \int_n^{n+1} x^{-(s'+1)}\, dx \end{aligned}$$

But
$$|x^{-(s'+1)} = x^{-(\sigma'+1)}.$$

Hence
$$\begin{aligned} |n^{-s'} - (n+1|^{-s'}| &\le |s'| \int_n^{n+1} x^{-(\sigma'+1)}\, dx \\ &= \frac{|s'|}{\sigma'} \left(n^{-\sigma'} - (n+1)^{-\sigma'} \right). \end{aligned}$$

Thus

$$\sum_{M}^{N} |n^{-s'} - (n+1)^{-s'}| \leq \frac{|s'|}{\sigma'} \left(M^{-\sigma'} - (N+1)^{-\sigma'} \right);$$

and so

$$\sum |n^{-s'} - (n+1)^{-s'}|$$

is convergent.

(b) *If*

$$\sigma = \Re(s)$$

then

$$|n^{-s}| = n^{-\sigma}.$$

But if $\sigma > 1$,

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

converges, by comparison with

$$\int x^{-\sigma}\, dx = \frac{1}{\sigma - 1} \, [x^{-(\sigma-1)}].$$

On the other hand, if $\sigma < 1$ then

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

diverges, by comparison with

$$\int x^{-1}\, dx = [\log x].$$

We conclude that the abscissa of convergence for $\zeta(s)$ is $\sigma = 1$.

(c) *We have*

$$f(s) = \left(1 - 2\, 2^{-s}\right) \zeta(s) = 1 - 2^{-s} + 3^{-s} - 4^{-s} + \cdots .$$

Now $f(\sigma)$ converges for real $\sigma > 0$, since the terms of the series are monotone decreasing and tend to 0.

On the other hand $f(\sigma)$ is not convergent for $\sigma < 0$ since the terms do not tend to 0.

It follows that the abscissa of convergence of $f(s)$ is $\sigma = 0$. Hence $f(s)$ is holomorphic in $\Re(s) > 0$; so

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \, f(s)$$

defines the analytic continuation of $\zeta(s)$ *to the region.*
The function

$$1 - 2^{1-s} = 1 - e^{(1-s)\log 2}$$

has zeros wherever

$$(1-s)\log 2 = 2n\pi i,$$

ie

$$s = 1 + \frac{2n\pi}{\log 2}\, i$$

(with $n \in \mathbb{Z}$*).*
On the fact of it, $\zeta(s)$ *could have poles at these points. However, we can consider the function*

$$g(s) = \left(1 - 3\, 3^{-s}\right)\zeta(s) = 1 + 2^{-s} - 2 \cdot 3^{-s} + 4^{-s} + 5^{-s} - 2 \cdot 6^{-s} + \cdots .$$

This series also converges for $\Re(s) > 0$*, on taking the terms three at a time. It follows that*

$$\zeta(s) = \frac{1}{1 - 3^{1-s)}}\, g(s)$$

also defines the analytic continuation of $\zeta(s)$*.*
Since

$$1 - 3^{1-s} = 1 - e^{(1-s)\log 3}$$

has zeros where

$$(1-s)\log 3 = 2m\pi i,$$

ie

$$s = 1 + \frac{2m\pi}{\log 3}\, i.$$

(with $n \in \mathbb{Z}$*).*
These two sets overlap where

$$\frac{n}{\log 2} = \frac{m}{\log 3}$$

ie

$$2^m = 3^n.$$

The only solution of this is $m = n = 0$*. It follows that* $\zeta(s)$ *can only have a pole in* $\Re(s) > 0$ *at the point* $s = 1$*.*
It does have a pole there, since

$$\zeta(\sigma) \to \infty \text{ as } \sigma \to 1+$$

(ie as $\sigma \to 1$ *from above).*

(d) *The technique could be used to continue* $\zeta(s)$ *to the whole complex plane. Thus*

9. State the Prime Number Theorem, and sketch its proof.

Answer:

(a) *The Prime Number Theorem states that*

$$\pi(x) \sim Li(x),$$

where $\pi(x)$ *is the number of primes* $\leq x$ *and*

$$Li(x) = \int_e^x \frac{dt}{\log t}.$$

(b) *The steps in the proof of the PNT are:*

Lemma 15.

$$Li(x) \sim \frac{x}{\log x}$$

This is a simple exercise in integration by parts.

Lemma 16. *The Riemann zeta function*

$$\zeta(s) = \sum n^{-s}$$

is holomorphic in $\Re(s) > 1$*, and can be extended to a meromorphic function in* $\Re(s)$ *with a single simple pole at* $s = 1$.

Lemma 17. *If* $\Re(s) > 1$,

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

Corollary 3. $\zeta(s)$ *has no zeros in* $\Re(s) > 1$.

Lemma 18. *If* $\Re(s) > 1$,

$$\begin{aligned} \frac{\zeta'(s)}{\zeta(s)} &= \sum \log p \, p^{-s} + h(s) \\ &= \int x^{-s} \, d\theta(x) + h(s), \end{aligned}$$

where

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

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

Lemma 19. *The PNT is equivalent to*

$$\theta(x) \sim x,$$

or equivalently

$$\psi(x) = o(x),$$

where

$$\psi(x) = \theta(x) - x.$$

This is proved using Riemann-Stieltjes integration by parts.

Lemma 20. *$\zeta(s)$ has no zeros on $\Re(s) = 1$.*

This is derived from the inequality

$$\cos 2t + 4\cos t + 3 \geq 0$$

which implies that

$$|\zeta(\sigma + 2ti)|\ |\zeta(\sigma + ti)|^4\ |\zeta(\sigma)|^3 \geq 1.$$

Lemma 21.

$$\Psi(s) = \int_1^\infty x^{-s} d\psi(x)$$

is holomorphic in $\Re(s) \geq 1$ (ie in some open set containing this region).

Corollary 4.

$$\Psi(s+1) = \int_1^\infty x^{-(s+1)}\ d\psi(x)$$

is holomorphic in $\Re(s) \geq 0$.

Lemma 22. *The Tauberian theorem: if $f(x)$ is bounded on $(0, \infty)$ then*

$$F(s) = \int_0^\infty e^{-xs} f(x)\ dx$$

is holomorphic in $\Re(s) > 0$. Furthermore, if $F(s)$ is holomorphic in $\Re(s) \geq 0$ then

$$\int_0^\infty f(x)\ dx = F(0).$$

Corollary 5. *If $g(x)$ is bounded on $(1,\infty)$ then*

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

is holomorphic in $\Re(s) > 0$. Furthermore, if $G(s)$ is holomorphic in $\Re(s) \geq 0$ then

$$\int_1^\infty g(x)\,\frac{dx}{x} = G(0).$$

This 'Mellin form' of the Tauberian theorem follows at once from the previous version on making the change of variable $y = e^x$ (and changing back from y to x).

Lemma 23.

$$\theta(x) = O(x).$$

This 'bootstrap lemma' follows on considering the primes dividing the binomial coefficient $\binom{2n}{n}$.

Corollary 6.

$$x^{-1}\psi(x)$$

is bounded.

Lemma 24. *The integral*

$$\int_1^\infty \frac{\psi(x)}{x^2}\,dx$$

converges.

[On integrating by parts,

$$\begin{aligned}
\Psi(s+1) &= \int_1^\infty x^{-(s+1)}\,d\psi(x)\\
&= \left[x^{-(s+1)}\psi(x)\right]_1^\infty + (s+1)\int_1^\infty x^{-(s+2)}\psi(x)\,dx\\
&= -1 + (s+1)\int_1^\infty x^{-(s+2)}\psi(x)\,dx
\end{aligned}$$

if $\Re(s) > 0$, since $\psi(x)/x$ is bounded as $x \to \infty$, while $x^{-s} \to 0$. Thus

$$\int_1^\infty x^{-(s+2)}\psi(x)\,dx = \frac{\Psi(s+1)+1}{s+1},$$

and the Tauberian Theorem can be applied.]

Lemma 25.

$$\int^{\infty} \frac{\psi(x)}{x^2}\, dx \text{ convergent } \implies \theta(x) \sim x.$$

This is a little tricky. It follows because $\psi(x)$ is not changing rapidly; so if $\psi(X) > C > 0$ then $\psi(x) > C/2$ for $x \in [X, X']$, where the interval is long enough to contribute $> C'$ to the integral, which will contradict convergence if it happens infinitely often; and similarly if $\psi(X) < -C < 0$.

Remarks. The two main steps in the proof are:

i. establishing that $\zeta(s)$ has no zeros on $\Re(s) = 1$; and

ii. the Tauberian theorem.