Course 2316 — Sample Paper 3

Timothy Murphy

April 20, 2015

The exam will last for 2 hours.
Attempt 5 questions. All carry the same mark.

1. Show that
$$\sum_{p \text{ prime}} \frac{1}{p}$$
is divergent. **Answer:**

By the Fundamental Theorem, each integer $n \geq 1$ is expressible in the form
$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots ,$$
where the sum extends over the primes, and $e_p \in \mathbb{N}$, with all but a finite number of the $e_p = 0$.

Inverting,
$$\frac{1}{n} = \frac{1}{2^{e_2}} \frac{1}{3^{e_3}} \frac{1}{5^{e_5}} \cdots .$$
Informally, by addition,
$$\begin{aligned}\sum_{n \in \mathbb{N}} \frac{1}{n} &= \sum_{e_2 \in \mathbb{N}} \frac{1}{2^{e_2}} \sum_{e_3 \in \mathbb{N}} \frac{1}{3^{e_3}} \sum_{e_5 \in \mathbb{N}} \frac{1}{5^{e_5}} \cdots \\ &= (1 - 1/2)^{-1} (1 - 1/3)^{-1} (1 - 1/5)^{-1} \cdots \\ &= \prod_p \frac{1}{1 - 1/p}.\end{aligned}$$
Formally,
$$\sum_{n \leq N} \frac{1}{n} \leq \prod_{p \leq N} \frac{1}{1 - 1/p},$$
since the primes dividing n are all $\leq n$.

We know that
$$\sum_{n \in \mathbb{N}} \frac{1}{n}$$

is divergent. It follows that

$$\prod_{p \le N} \frac{1}{1 - 1/p} \to \infty$$

as $N \to \infty$.

Thus, taking logarithms,

$$\sum_p \ln\left(\frac{1}{p-1}\right) = \sum_p \ln\left(1 + \frac{1}{p-1}\right)$$

diverges.

But

$$\ln(1 + x) \le x$$

if $x \ge 1$; *for if*

$$f(x) = \ln(1 + x) - x$$

then

$$f'(x) = \frac{1}{1+x} - 1 = -\frac{x}{1+x} \le 0.$$

It follows that

$$\sum_p \frac{1}{p-1}$$

diverges, and so therefore does

$$\sum_p \frac{1}{p},$$

since $p_n - 1 \ge p_{n-1}$.

2. How many numbers between 1 and 1 million are not divisible by any of the 10 integers $1 - 10$?

   Answer: Lemma. Suppose X is a finite set, and suppose

   $$S_i \subset X$$

   for $i = 1, \ldots, r$. Then

   $$\#(S_1 \cup S_2 \cup \cdots \cup S_r) =$$
   $$\sum_i \#(S_i) - \sum_{i,j} \#(S_i \cap S_j) + \sum_{i,j.k} \#(S_i \cap S_j \cap S_k) - \sum_{i,j.k.l} \#(S_i \cap S_j \cap S_k \cap S_l) + \cdots.$$

We use this lemma to determine the size of the complementary set S, ie the numbers in $[1, 10^6]$ divisible by one of 2–10, or in other words by 2,3,5, or 7.

If we set

$$T_m = \{n \in [1, 10^6] : m|n\}$$

then

$$S = T_2 \cup T_3 \cup T_5 \cup T_7;$$

Also

$$T_m = [10^6/m],$$

where $[x]$ is the largest integer $\le x$; and if $\gcd(m, n) = 1$ then

$$T_m \cap T_n = T_{mn}.$$

Hence, by the Lemma,

$$\begin{aligned}\#S &= \#T_2 + \#T_3 + \#T_5 + \#T_7 \\ &\quad - \#T_6 - \#T_{10} - \#T_{14} - \#T_{15} - \#T_{21} - \#T_{35} \\ &\quad + \#T_{30} + \#T_{42} + \#T_{70} + \#T_{105} \\ &\quad - \#T_{210} \\ &= 500,000 + 333,333 + 200,000 + 142,857 \\ &\quad - 166,666 - 100,000 - 71,428 - 66,666 - 47,619 - 28,571 \\ &\quad + 33,333 + 23,809 + 14,285 + 9,523 \\ &\quad - 4,761 \\ &= (500,000+200,000-100,000+333,333-33,333)+(142,857-71,428) \\ &\quad -(166,666+66,666)-(47,619-23,809)-(28,571-14,285)+(9,523-4,761) \\ &= 900,000 + 71,429 - 233,332 - 23,810 - 14,286 + 4,762 \\ &= 976,191 - 271,428 \\ &= 704,763.\end{aligned}$$

Thus the number not *divisible by 1–10 is*

$$1,000,000 - 704,763 = 295,237.$$

[Nb: I have not checked my arithmetic!]

3. State (without proof) the Prime Number Theorem.

   Show that the theorem implies that

$$p_n \sim n \log n,$$

   where p_n is the nth prime.

   Answer:

(a) **Theorem.**

$$\pi(x) \sim \frac{\ln x}{x},$$

where $\pi(x)$ denotes the number of primes $\leq x$.

(b) *By definition*

$$\pi(p_n) = n.$$

Let

$$f(x) = \frac{x}{\ln x}, \quad g(x) = x \ln x.$$

Then

$$\begin{aligned} g(f(x)) &= \frac{x}{\ln x}(\ln x - \ln\ln x) \\ &= x\frac{\ln x}{\ln x - \ln\ln x} \\ &\sim x, \end{aligned}$$

while

$$\begin{aligned} f(g(x)) &= \frac{x\ln x}{\ln x + \ln\ln x} \\ &= x\frac{\ln x}{\ln x + \ln\ln x} \\ &\sim x. \end{aligned}$$

Hence

$$\pi(x) \sim f(x) \implies g(\pi(x)) \sim g(f(x)) \sim x.$$

In particular, setting $x = p_n$*,*

$$g(n) \sim p_n,$$

ie

$$p_n \sim n \ln n.$$

4. Find all the generators of the multiplicative group $(\mathbb{Z}/23)^{\times}$.

   Is the group $(\mathbb{Z}/25)^{\times}$ (formed by the invertible elements of $\mathbb{Z}/(25)$) cyclic? If so, find a generator.

   Answer:

   (a) *The group* $(\mathbb{Z}/23)^{\times}$ *has 22 elements, so the order of each element divides 22, by Lagrange's Theorem, ie the order is 1,2,11 or 22. Evidently* $2^2 \not\equiv 1 \bmod 23$*. So 2 has order 11 or 22* $\bmod 23$.

We have

$$2^6 = 64 \equiv -5 \bmod 23,$$

so

$$2^{12} \equiv 25 \equiv 2 \bmod 23.$$

Since $\gcd(2, 23) = 1$*, we can divide by 2, and so*

$$2^{11} = 1 \bmod 23.$$

Thus 2 has order 11 mod 23.
Since

$$(-2)^{11} \equiv -2^{11} \equiv -1 \bmod 23,$$

it follows that -2 *has order 22* $\bmod 23$*, ie* -2 *generates the group, which is therefore cyclic [as of course we know].*

Lemma. If g is a generator of the cyclic group C_n then g^r is also a generator if and only if $\gcd(r, n) = 1$.

It follows that the generators of $(\mathbb{Z}/23)^\times$ *are*

$$(-2)^r \bmod 23 \qquad (r = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21).$$

Now we know that

$$(-2)^r \equiv -2^r \bmod 23$$

if r *is odd, while*

$$2^{11} \equiv 1 \bmod 23.$$

Hence

$$\begin{aligned}
(-2)^3 &\equiv -8 \bmod 23,\\
(-2)^5 &\equiv -32 \equiv -9 \bmod 23,\\
(-2)^7 &\equiv 4 \cdot -9 = -36 \equiv 10 \bmod 23,\\
(-2)^9 &\equiv 4 \cdot 10 = 40 \equiv -6 \bmod 23,\\
[(-2)^{11} &\equiv 4 \cdot -6 \equiv -1 \bmod 23,]\\
(-2)^{13} &\equiv 4 \cdot -1 = -4 \bmod 23,\\
(-2)^{15} &\equiv 4 \cdot -4 = -16 \equiv 7 \bmod 23,\\
(-2)^{17} &\equiv 4 \cdot 7 = 28 \equiv 5 \bmod 23,\\
(-2)^{19} &\equiv 4 \cdot 5 = 20 \equiv -3 \bmod 23,\\
(-2)^{21} &\equiv 4 \cdot -3 = -12 \equiv 11 \bmod 23,\\
[(-2)^{22} &\equiv -2 \cdot 11 = -22 \equiv 1 \bmod 23.]
\end{aligned}$$

Thus the generators of the group are:

$$5, 7, 10, 11, -2, -3, -4, -6, -8, -9 \bmod 23.$$

(b) *The group* $(\mathbb{Z}/25)^\times$ *has order*

$$\phi(5^2) = 5 \cdot 4 = 20.$$

Evidently $(\mathbb{Z}/5)^\times$ *is cyclic, with generators* ± 2.
Thus 2 has order $4 \bmod 5$*; so its order* $\bmod 25$ *is a multiple of 4. On the other hand the order must divide 20. Hence it is either 4 or 20.*
Now

$$2^4 = 16 \not\equiv 1 \bmod 25.$$

Hence 2 has order $20 \bmod 25$, *ie it is a generator of* $(\mathbb{Z}/25)^\times$, *which is therefore cyclic.*

5. 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

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

Answer:

(a) *Let*

$$f(x) = x^r + 1.$$

If r *is odd then*

$$f(-1) = 0.$$

It follows that

$$x + 1 \mid f(x).$$

In fact

$$f(x) = (x+1)(x^{r-1} - x^{r-2} + \cdots - x + 1).$$

If now m *has an odd factor* r, *say*

$$m = rs,$$

then it follows on setting $x = 2^s$ *that*

$$2^s + 1 \mid 2^m + 1.$$

Hence m *has no odd factors if* $2^m + 1$ *is prime, ie*

$$m = 2^n.$$

(b) Suppose

$$F_n = 2^{2^n} + 1 \quad (n > 0)$$

is prime.
Then

$$F_n \equiv 1 \bmod 4.$$

It follows from Gauss' Reciprocity Theorem that

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

Now

$$2^{2^n} \equiv (-1)^{2^n} \equiv 1 \bmod 3,$$

and so

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

It follows that

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

But by Eisenstein's Criterion,

$$3^{(N-1)/2} \equiv \left(\frac{3}{F_n}\right) = -1 \bmod F_n,$$

ie

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

Conversely, suppose this result holds. Since $F_n \equiv 2 \bmod 3$, *it must have a prime factor*

$$P \equiv 2 \bmod 3;$$

and then

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

It follows that the order of $3 \bmod P$ *must be exactly* 2^{2^n}. *For certainly*

$$3^{2^{2^n}} = (3^{2^{2^n-1}})^2 \equiv 1 \bmod P.$$

So the order divides 2^{2^n}, *and is therefore a power of 2. But the order cannot be smaller than* 2^{2^n} *since*

$$3^{2^{2^n-1}} \not\equiv 1 \bmod P.$$

By Fermat's Little Theorem,

$$2^{2^n} | P - 1.$$

Hence

$$2^{2^n} \leq P - 1.$$

ie

$$P \geq 2^{2^n} + 1 = F_n.$$

It follows that

$$P = F_n,$$

ie F_n is prime.

6. Suppose

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

where m is odd. Show that if n is prime, and a is coprime to n, then either

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

or else

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

for some $f \in [0, e)$.

Show conversely that if this is true for all a coprime to n then n is prime.

Answer:

(a) *Suppose n is prime. Then*

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

by Fermat's Little Theorem. Thus

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

and so

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

If

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

we are done; otherwise

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

and so

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

Continuing in this way, we see that either

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

at some stage, or else we conclude with

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

(b) *Suppose now that n is not prime, but that all a coprime to n have the above property.*

Then n has at least two prime factors. Let us suppose first that it has two distinct prime factors, p and q.

We are going to consider the orders of a modulo p, q, n. But we are only interested in the power of 2 dividing the order, in each case. Suppose $g \in G$ has order $2^f m$, where m is odd. Let us call f the 2-order of g, and write

$$O_2(g, n) = f.$$

[Nb: This is not a standard notation.]

Lemma. Suppose

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

Then

$$O_2(a, n) = f + 1.$$

For certainly

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

and so

$$O_2(a, n) \leq f + 1.$$

On the other hand, if

$$O_2(a, n) = f' \leq f,$$

so the order of $a \bmod n$ *is* $2^{f'}m'$*, where* m' *is odd, then*

$$\begin{aligned} 2^{f'}m' \mid 2^{f+1}m &\implies m' \mid m \\ &\implies a^{2^f m} \equiv 1 \bmod n, \end{aligned}$$

contrary to the supposition that

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

Hence

$$O_2(a, n) = f + 1.$$

Now suppose

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

Then

$$a^{2^f m} \equiv -1 \bmod p \text{ and } a^{2^f m} \equiv -1 \bmod q.$$

It follows from the lemma that

$$O_2(a, n) = O_2(a, p) = O_2(a, q) = f + 1.$$

Lemma. If p is an odd prime, the group $(\mathbb{Z}/p)^\times$ is cyclic.
It follows that we can find a *having any order* $\mid p - 1$ *modulo* p*, and any order* $\mid q - 1$ *modulo* q*.*
In particular, we can find an a *such that*

$$O_2(a, p) \neq O_2(a, q),$$

leading to a contradiction. It remains to consider the case when

$$n = p^r,$$

with $r \geq 2$*. In this case the group* $(\mathbb{Z}/n)^\times$ *has order*

$$\phi(p^r) = (p - 1)p^{r-1}.$$

It follows that we can find an element a *of order* p*. But our hypothesis implies that*

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

Thus

$$p \mid p^r - 1,$$

which is absurd.
We have shown that if all a *coprime to* n *have the specified property then* n *must be prime.*

[Note: Eisenstein's Criterion gives an alternative way of finding an a with

$$O_2(a, p) \neq O_2(a, q),$$

Suppose

$$p - 1 = 2^g r, \; q - 1 = 2^h s,$$

where r, s are odd.

By Eisenstein's Criterion,

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

Thus

$$\left(\frac{a}{p}\right) = -1 \implies a^{2^{g-1}} \equiv -1 \bmod p \implies O_2(a, p) = g.$$

On the other hand

$$\left(\frac{a}{p}\right) = 1 \implies a^{2^{g-1}} \equiv 1 \bmod p \implies O_2(a, p) < g.$$

But by the Chinese Remainder Theorem, we can choose $\left(\frac{a}{p}\right)$ and $\left(\frac{a}{q}\right)$ independently. In particular, we can find an a with

$$O_2(a, p) \neq O_2(a, q),$$

contradicting our hypothesis.]

7. State without proof Gauss' Quadratic Reciprocity Law.

   Does there exist a number n such that n^2 ends in the digits 1234? If so, find the smallest such n. **Answer:**

   (a) *If a is coprime to the prime p then we set*

   $$\left(\frac{a}{p}\right) = \begin{cases} +1 & \textit{if } a \textit{ is a quadratic residue} \bmod p, \\ -1 & \textit{if } a \textit{ is a quadratic non-residue} \bmod p. \end{cases}$$

   Gauss' Law states that if p, q are odd primes then

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

(b) *We have to determine if there is an integer n such that*

$$n^2 \equiv 1234 \bmod 10000.$$

By the Chinese Remainder Theorem this is equivalent to asking if each of the congruences

$$m^2 \equiv 1234 \bmod 2^5,$$
$$n^2 \equiv 1234 \bmod 5^5$$

is soluble.
The first is insoluble, since

$$m^2 \equiv 1234 \bmod 2^5 \implies m^2 \equiv 1234 \bmod 2^2,$$

and

$$1234 \equiv 2 \bmod 4,$$

while

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

Hence there is no such n.

8. What is meant by an *algebraic number* and by an *algebraic integer*?

   Show that the algebraic integers in the field $\mathbb{Q}(\sqrt{-3}$ form the ring $\mathbb{Z}[\omega]$, where $\omega = (1 + \sqrt{-3})/2/$

   Show that this ring is a unique factorisation domain, and determine the units and primes in this domain.

   Answer:

   (a) *An algebraic number is a number $\alpha \in \mathbb{C}$ satisfying a polynomial equation*

   $$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0,$$

   with $a_1, a_2, \ldots, a_n \in \mathbb{Q}$.

   (b) *An algebraic integer is a number $\alpha \in \mathbb{C}$ satisfying a polynomial equation*

   $$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0,$$

   with $a_1, a_2, \ldots, a_n \in \mathbb{N}$.

(c) The field $\mathbb{Q}(\sqrt{-3})$ *consists of the numbers*

$$z = x + y\sqrt{-3}$$

with $x, y \in \mathbb{Q}$*. If* z *satisfies the equation*

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0,$$

with $a_1, a_2, \ldots, a_n \in \mathbb{Q}$*, then so does*

$$\bar{z} = x - y\sqrt{-3}.$$

Lemma. The algebraic integers form a ring.
Lemma. If $\alpha \in \mathbb{Q}$ is an algebraic integer then $\alpha \in \mathbb{Z}$.
Suppose z *is an algebraic integer. Then so is* $\bar{z}$ *(since it satisfies the same polynomial equations over* $\mathbb{Q}$ *or* $\mathbb{Z}$*). It follows that*

$$z + \bar{z} = 2x$$

is an algebraic integer, and so

$$2x \in \mathbb{Z}.$$

Similarly,

$$z\bar{z} = x^2 + 3y^2 \in \mathbb{Z}.$$

Hence

$$\begin{aligned} 4x^2 + 12y^2 = (2x)^2 + 3(2y)^2 &\in \mathbb{Z} \\ \implies 3(2y)^2 &\in \mathbb{Z} \\ \implies 2y &\in \mathbb{Z}. \end{aligned}$$

Thus

$$x = a/2, \; y = b/2,$$

where $a, b \in \mathbb{Z}$ *and*

$$x^2 + 3y^2 = \frac{a^2 + 3b^2}{4} \in \mathbb{N}$$

ie

$$a^2 + 3b^2 \equiv 0 \bmod 4.$$

Hence either a, b *are both odd, or both even. It follows that*

$$z = c + d\frac{1 + \sqrt{-3}}{2} = c + d\omega,$$

with $c, d \in \mathbb{Z}$.
Conversely, ω *is an algebraic integer, since it satisfies the equation*

$$x^2 - x + 1 = 0.$$

Thus

$$z = c + d\omega$$

is an algebraic integer, since the algebraic integers form a ring.
Hence the algebraic integers in $\mathbb{Q}(\sqrt{-3})$ *are the numbers*

$$\{c + d\omega : c, d \in \mathbb{Z}\} = \mathbb{Z}[\omega].$$

(d) *If*

$$z = x + y\sqrt{-3} \quad (x, y \in \mathbb{Q})$$

we set

$$\mathcal{N}(z) = z\bar{z} = x^2 + 3y^2.$$

Evidently,

$$\mathcal{N}(zw) = \mathcal{N}(z)\,\mathcal{N}(w).$$

Now suppose $z, w \in \mathbb{Z}[\omega]$. *Let*

$$\frac{z}{w} = x + y\omega.$$

Choose $a, b \in \mathbb{Z}$ *such that*

$$|x - a| \leq 1/2, \; |y - b| \leq 1/2,$$

and let

$$q = a + b\omega.$$

Then

$$\frac{z}{w} - q = (x - a) + (y - b)\omega.$$

Hence

$$\mathcal{N}(\frac{z}{w} - q) = \frac{(x-a)^2 + 3(y-b)^2}{4} \leq \frac{1/4 + 3/4}{4} = \frac{1}{4} < 1.$$

Thus

$$\mathcal{N}(z - qw) < \mathcal{N}(w).$$

In other words, given $z, w \neq 0 \in \mathbb{Z}[\omega]$ *we can find* $q, r \in \mathbb{Z}[\omega]$ *such that*

$$z = qw + r,$$

with $\mathcal{N}(r) < \mathcal{N}(w)$.

This allows us to set up the Euclidean Algorithm:

$$\begin{aligned} z &= q_0 w + r_0, \\ w &= q_1 r_0 + r_1, \\ r_0 &= q_2 r_1 + r_2, \\ &\dots \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

The process must finish, since

$$\mathcal{N}(r_0) > \mathcal{N}(r_1) > \cdots > \mathcal{N}(r_n) > 0,$$

ie the norms form a decreasing sequence of positive integers.
It follows that

$$d = r_n = \gcd(z, w),$$

ie

$$d \mid z, w \text{ and } e \mid z, w \implies e \mid d.$$

Also, working backwards through the algorithm, we can find $u, v \in \mathbb{Z}[\omega]$ *such that*

$$uz + vw = d.$$

Recall that $\epsilon \in \mathbb{Z}[\omega]$ *is said to be a unit if it is invertible in* $\mathbb{Z}[\omega]$.
Lemma. ϵ is a unit if and only if $\mathcal{N}(\epsilon) = 1$.
For

$$\begin{aligned} \epsilon\theta = 1 &\implies \mathcal{N}(\epsilon)\mathcal{N}(\theta) = \mathcal{N}(1) = 1 \\ &\implies \mathcal{N}(\epsilon) = \mathcal{N}(\theta) = 1. \end{aligned}$$

Conversely

$$\mathcal{N}(\epsilon) = 1 \implies \epsilon\bar{\epsilon} = 1.$$

We say that π *is indecomposable if*

$$\pi = \sigma\tau$$

implies that σ *or tau is a unit.*
Now we can establish Euclid's Lemma: If π *is indecomposable then*

$$\pi \mid zw \implies \pi \mid z \text{ or } \pi \mid w.$$

Lemma. Suppose $z \in \mathbb{Z}[\omega]$. Then z is expressible as a product of indecomposables:

$$z = \pi_1 \cdots \pi_r.$$

This follows by induction on $\mathcal{N}(z)$. If z is indecomposable the result is trivial. Otherwise

$$z = uv,$$

where neither u nor v is a unit. Hence

$$\mathcal{N}(u), \mathcal{N}(v) > 1 \implies \mathcal{N}(u), \mathcal{N}(v) < \mathcal{N}(z),$$

so the inductive hypothesis can be applied to u, v, giving the result for z.

Finally, the uniqueness of the expression for z as a product of irreducibles (up to order and multiplication by units) follows from Euclid's Lemma. Again, we argue by induction on $\mathcal{N}(z)$. Suppose

$$z = \pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s'.$$

Then

$$\pi_1 \mid \pi_i'$$

for some i, by Euclid's Lemma; and uniqueness follows on applying the inductive hypothesis to

$$z/\pi_1 = \pi_2 \cdots \pi_r = \pi'1 \cdots \pi_{r-1}' \pi_{r+1}' \cdots \pi_s'.$$

(e) *We have seen that*

$$\epsilon = a + b\omega$$

is a unit if and only if

$$\mathcal{N}(\epsilon) = (a + b\omega)(a + b\bar{\omega}) \quad = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2 \quad = 1.$$

In other words,

$$(a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 = 1,$$

ie

$$(2a - b)^2 + 3b^2 = 4.$$

Evidently the only solutions to this are

$$(2a - b, b) = (\pm 2, 0) \text{ or } (\pm 1, \pm 1),$$

giving

$$(a,b) = \pm(1,0),\ \pm(1,1),\ \pm(0,1).$$

Since $1+\omega = -\omega^2$, *it follows that* $\mathbb{Z}[\omega]$ *has just 6 units:*

$$\pm 1,\ \pm\omega,\ \pm\omega^2.$$

(f) *Since we have established unique factorisation, we may refer to indecomposables as 'primes', with the understanding that we do not distinguish between* π *and* $\epsilon\pi$, *where* ϵ *is a unit.*
Suppose π *is prime. Let*

$$\mathcal{N}(\pi) = \pi\bar{\pi} = p_1 \dots p_r,$$

where the p_i *are rational primes. Then*

$$\pi \mid p_i$$

for some p_i.
So every prime π *divides a rational prime* p. *Hence*

$$\mathcal{N}(\pi) \mid \mathcal{N}(p) = p^2.$$

Thus

$$\mathcal{N}(\pi) = p \text{ or } p^2.$$

If $\mathcal{N}(\pi) = p^2$ *then*

$$p = \epsilon\pi,$$

ie the rational prime p *does not split in* $\mathbb{Z}[\omega]$.
If $\mathcal{N}(\pi) = p$ *then*

$$p = \pi\bar{\pi},$$

ie p *splits into two primes.*
Evidently,

$$3 = -(\sqrt{-3})^2,$$

so 3 ramifies.
Thus we may assume that $p \neq 3$.
Suppose

$$p = \pi\bar{\pi},$$

where

$$\pi = a + b\omega.$$

Then

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

Note that if $p = 2$ then a, b must both be even, in which case the left-hand side is divisible by 4, which is impossible. So 2 does not split in $\mathbb{Z}[\omega]$, and we may assume that $p \neq 2, 3$.

Now

$$a^2 + ab + b^2 \equiv 0 \bmod p,$$

and so

$$(2a - b)^2 + 3b^2 \equiv 0 \bmod p.$$

But this implies that -3 is a quadratic residue mod p*, since b is evidently coprime to p, ie*

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

But

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

and

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

Also, by Gauss' Reciprocity Theorem,

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

while

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

Putting all these together, we see that

$$\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 5, 19, 23 \bmod 24, \\ -1 & \text{if } p \equiv 7, 11, 13, 17 \bmod 24. \end{cases}$$

ie

$$\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1, \pm 5 \bmod 24, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \bmod 24. \end{cases}$$

Finally, suppose

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

ie -3 *is a quadratic residue* mod p. *Then we can a coprime to* p *such that*

$$a^2 + 3 \equiv 0 \bmod p,$$

ie

$$a^2 + 3 = pq$$

ie

$$(a + \sqrt{-3})(a - \sqrt{-3}) = pq.$$

If now p *remains prime in* $\mathbb{Z}[\omega]$ *then since there is unique factorisation in this ring it follows that*

$$p \mid (a + \sqrt{-3}) \text{ or } p \mid (a - \sqrt{-3})$$

both of which imply that $p \mid 1$, *which is absurd.*
We conclude that the rational prime $p \neq 2, 3$ *splits in* $\mathbb{Z}[\omega]$ *if and only if*

$$p \equiv \pm 1, \pm 5 \bmod 24.$$

We should consider finally if the prime p *ramifies in any of these cases, ie if*

$$\bar{\pi} = \epsilon \pi,$$

where $\epsilon \in \{\pm 1, \pm \omega, \pm \omega^2\}$.
If this is so, then (multiplying by π*),*

$$p = \epsilon \pi^2.$$

Suppose

$$\pi = a + b\omega.$$

Then

$$\begin{aligned}\pi^2 &= (a+b\omega)^2\\ &= a^2 + ab\omega + b^2\omega^2\\ &= (a^2-b^2) + (ab-b^2)\omega.\end{aligned}$$

Thus

$$\begin{aligned}p \mid \pi^2 &\implies ab - b^2 = b(a-b) \equiv 0 \bmod p\\ &\implies a \equiv b \bmod p\\ &\implies p = a^2 - ab + b^2 \equiv a^2 \bmod p\\ &\implies p \mid a,\end{aligned}$$

contradicting the fact that a is coprime to p.
We have shown therefore that in $\mathbb{Z}[\omega]$

i. *$p = 3$ ramifies;*
ii. *if $p = 2$ or $p \equiv \pm 7, \pm 11 \bmod 24$ then p remains prime;*
iii. *if $p \equiv \pm 1, \pm 5 \bmod 24$ then p splits into 2 distinct primes.*