Course 2316 — Sample Paper 1

Timothy Murphy

April 19, 2015

Attempt 5 questions. All carry the same mark.

1. State and prove the Fundamental Theorem of Arithmetic (for $\mathbb{N}$).

   Prove that there are an infinity of primes $\equiv 3 \bmod 4$.

   What can you say about primes $\equiv 1 \bmod 4$?

   Answer:

   (a) *The integer $p > 1$ is said to be* prime *if its only factors are 1 and p itself.*

   Theorem. Each integer $n > 1$ is expressible as a product of primes,

   $$n = p_1 \dots p_r,$$

   and the expression is unique up to order.

   Proof. We say that $m, n \in \mathbb{Z}$ are coprime if the only common factor they have is 1.

   Lemma. *If m, n are coprime then we can find $x, y \in \mathbb{Z}$ such that*

   $$mx + ny = 1.$$

   Proof. The result is trivial if $m = 0$ or $n = 0$, so we may assume $m, n > 0$. Consider the set of integers

   $$S = \{mx + ny : x, y \in \mathbb{Z}\}.$$

   Let d be the smallest integer > 0 in this set. Divide m by d:

   $$m = qd + r,$$

   where $0 \leq r < d$.
   Then $r \in S$. Hence $r = 0$ by the minimality of d, ie $d \mid m$.
   Similarly $d \mid n$. Hence $d = 1$ since m, n are coprime. □

Lemma. *[Euclid's Lemma] Suppose p is prime, and $a, b \in \mathbb{Z}$. Then*

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proof. Suppose $p \nmid a$. Then a, p are coprime, and so there exist $x, y \in \mathbb{Z}$ such that

$$ax + py = 1.$$

Multiplying by b,

$$abx + pby = b \implies p \mid b,$$

since p divides both terms on the left. □

Lemma. *Every $n > 1$ is a product of primes.*

Proof by induction on n. Suppose n is not a prime. Then $n = ab$, with $1 < a, b < n$. Both a and b are expressible as products of primes, by the inductive hypothesis. Hence so is n. □

Lemma. *The expression for $n > 1$ as a product of primes is unique up to order.*

Proof by induction on n. Suppose

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

are two expressions for n as products of primes. By repeated application of Euclid's Lemma,

$$p_1 \mid q_j$$

for some j. Since q_j is prime, it follows that

$$p_1 = q_j.$$

Thus

$$\frac{n}{p_1} = p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s;$$

and the result follows from the inductive hypothesis. □

□

(b) *Suppose the only primes* $\equiv 3 \bmod 4$ *are*

$$p_1, \ldots, p_r.$$

Let

$$N = 4p_1 \cdots p_r - 1.$$

Note that

$$N \equiv 3 \bmod 4.$$

By the Fundamental Theorem,

$$N = q_1 \cdots q_s$$

where the q's are primes.
Then one (at least) of these primes, q_j *say, must be* $\equiv 3 \bmod 4$. *For*

$$q_1 \equiv \cdots \equiv q_s \equiv 1 \bmod 4 \implies N \equiv 1 \bmod 4.$$

Thus

$$q_j = p_i$$

for some i. *But this implies that*

$$p_i | N,$$

which is impossible since

$$N \equiv -1 \bmod p_i.$$

(c) *By Dirichlet's Theorem, there are an infinity of primes* $\equiv 1 \bmod 4$. *In fact, if* $\pi_1(n), \pi_3(n)$ *are the number of primes* $p \leq n$ *congruent, respectively, to 1 and 3* mod4 *then*

$$\pi_1(n) \sim \pi_3(n) \sim \frac{n}{2 \ln n}$$

as $n \to \infty$.

2. Given $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$ and $r, s \in \mathbb{Z}$, prove that there exists $x \in \mathbb{Z}$ such that

$$x \equiv r \bmod m, \quad x \equiv s \bmod n.$$

Find the smallest positive integer x such that

$$x \equiv 3 \bmod 5, \ x \equiv 7 \bmod 11, \ x \equiv 12 \bmod 13.$$

Find the largest integer x *not* expressible in the form

$$x = 7a + 11b$$

with $a, b \geq 0$.

Answer:

(a) Consider the group homomorphism

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

This homomorphism is injective; for

$$\begin{aligned} x \in \ker \Theta &\implies m \mid x,\ n \mid x \\ &\implies mn \mid x \\ &\implies x = 0 \bmod mn. \end{aligned}$$

Since $\mathbb{Z}/(mn)$ and $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ both contain mn elements, Θ is bijective.
In particular, it is surjective; and so we can find $x \in \mathbb{Z}/(mn)$ such that

$$\Theta(x) = (r \bmod m,\ s \bmod n).$$

(b) Let us find u, v, w such that

$$u \equiv 1 \bmod 5,\ u \equiv 0 \bmod 11,\ u \equiv 0 \bmod 13;$$
$$v \equiv 0 \bmod 5,\ v \equiv 1 \bmod 11,\ v \equiv 0 \bmod 13. w \equiv 0 \bmod 5,\ w \equiv 0 \bmod 11,\ w \equiv 1 \bmod 1$$

For the first,

$$11 \cdot 13 = 143 \equiv 3 \bmod 5,$$

so we can take

$$u = 2 \cdot 11 \cdot 13 = 286.$$

For the second,

$$5 \cdot 13 = 65 \equiv -1 \bmod 11,$$

so we can take

$$v = -5 \cdot 13 = -65.$$

For the third,

$$5 \cdot 11 = 55 \equiv 4 \bmod 13,$$

so we can take

$$w = -3 \cdot 5 \cdot 11 = -165.$$

Thus a solution to the 3 simultaneous congruences is

$$\begin{aligned} x &= 3u - 4v - w, \\ &= 858 + 260 + 165 \\ &= 1283. \end{aligned}$$

The general solution is

$$1283 + 5 \cdot 11 \cdot 13t = 1283 + 715t.$$

Thus the smallest positive solution is

$$x = 1283 - 715 = 568.$$

(c) *Since* $\gcd(7, 11) = 1$ *we can find* $x, y \in \mathbb{Z}$ *such that*

$$7x + 11y = 1.$$

In fact

$$7 \cdot 3 = 21 \equiv -1 \bmod 11,$$

so we can take

$$x = -3,\ y = 2.$$

Thus for any n*,*

$$n = 7(-3n) + 11(2n).$$

The general solution to

$$n = 7u + 11v$$

is

$$n = 7(-3n + 11t) + 11(2n - 7t),$$

with $t \in \mathbb{Z}$*.*
If now

$$n \geq 7 \cdot 11$$

then we can choose t *so that*

$$0 \leq -3n + 11t < 11,$$

and then

$$7(-3n + 11t) < 7 \cdot 11 \implies 2n - 7t > 0.$$

We have shown therefore that the equation

$$n = 7a + 11b$$

has a solution with $a, b \geq 0$ *if* $n \geq 7 \cdot 11$*. Obviously there is no such solution if* $n = 1$*, so the greatest* n *with no solution lies between 1 and 76.*

3. Show that if

$$M = a^e - 1 \quad (a, e > 1)$$

is prime then $a = 2$ and e is prime.

Find the smallest number

$$M = 2^p - 1$$

(with p prime) that is *not* prime.

Answer:

(a) Suppose $a > 2$. We know that

$$x - 1 \mid x^e - 1.$$

In fact

$$x^e - 1 = (x - 1)(x^{e-1} + x^{e-2} + \cdots 1)$$

Substituting $x = a$ we see that

$$a - 1 \mid a^e - 1.$$

Now suppose e is not a prime, say

$$e = cd,$$

where $c, d > 1$.
Then as above,

$$x - 1 \mid x^d - 1.$$

Substituting $x = a^c$,

$$a^c - 1 \mid (a^c)^d - 1 = a^e - 1.$$

(b) Evidently,

$$2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31,\ 2^7 - 1 = 127$$

are all prime.
Since $2^{10} = 1024$,

$$2^{11} - 1 = 2047.$$

If this is prime then

$$a^{2046} \equiv 1 \bmod 2047$$

for $a = 1, 2, \ldots, 2046$. by Fermat's Little Theorem. In other words, the order of $a \bmod 2047$ must divide 2046.
But the order of $2 \bmod 2047$ is 11, which does not divide 2046. Hence

$$M_{11} = 2^{11} - 1$$

is not prime.

4. Prove that if p is an odd prime, then the multiplicative group $(\mathbb{Z}/p)^\times$ is cyclic.

   Find the orders of all the elements of $(\mathbb{Z}/17)^\times$.

   Answer:

   (a) *Recall that the* exponent *e of a finite group G is the smallest number $e > 1$ such that $g^e = 1$ for all $g \in G$. In other words, e is the lcm of the orders of the elements of G.*

   By Lagrange's Theorem, $e \mid n$, the order of G.

   Lemma. If A is a finite abelian group, and the elements $a, b \in A$ have coprime orders m, n then the order of ab is mn.

   Proof. Suppose the order of ab is d. Then

$$d \mid mn$$

   since

$$(ab)^{mn} = a^{mn}b^{mn} = 1.$$

   On the other hand,

$$\begin{aligned} (ab)^d = 1 &\implies (ab)^{dn} = 1 \\ &\implies a^{dn}b^{dn} = 1 \\ &\implies a^{dn} = 1 \\ &\implies m \mid dn \\ &\implies m \mid d, \end{aligned}$$

   since m, n are coprime. Similarly

$$n \mid d.$$

   Hence

$$mn \mid d,$$

   since m, n are coprime.

   Thus

$$d = mn.$$

   □

   Lemma. If the exponent of the finite abelian group A is e then there is an element $a \in A$ of exponent e.

Proof. Suppose

$$e = p_1^{e_1} \cdots p_r^{e_r}.$$

For each i, $1 \leq i \leq n$, there must be an element a_i whose order is divisible by $p_i^{e_i}$. (Otherwise the lcm of the orders would contain p_i to a lower power.)
Suppose the order of a_i is $p_i^{e_i} q_i$. Then the order of

$$b_i = a_i^{q_i}$$

is $p_i^{q_i}$.
Hence by the last Lemma, the order of

$$a = b_1 \cdots b_r$$

is e. □

Lemma. If F is a finite field of order n then the exponent e of the multiplicative group F^* satisfies

$$e = n - 1.$$

Proof. We have

$$x^e = 1$$

for all $x \neq 0$ in F. Thus the polynomial

$$f(x) = x^e - 1$$

of degree e in $F[x]$ has at least $n - 1$ distinct roots.
But a polynomial of degree e has at most e roots. Hence

$$e \leq n - 1.$$

On the other hand,

$$e \mid n - 1$$

by Lagrange's Theorem.
Hence

$$e = n - 1.$$

□

It follows from the last Lemma that the exponent of $(\mathbb{Z}/p)^*$ *is* $p-1$. *But then, from the previous Lemma, there is an element in the group of order* $p - 1$. *Hence the group is cyclic.*

(b) *Recall that if A is a cyclic group of order n, and $d \mid n$, then:*

i. *There is just one subgroup of order d, it is cyclic, and consists of all elements of order $r \mid n$;*
ii. *There are $\phi(d)$ elements of order d in A.*
iii. *If g generates A then g^r generates A if and only if* $\gcd(n, r) = 1$.

The order of each element of $(\mathbb{Z}/17)^*$ divides $17-1 = 16$, in other words the order is 1,2,4,8 or 16.
Evidently

$$2^4 \equiv -1 \bmod 17 \implies 2^8 \equiv 1 \bmod 17.$$

Hence 2 has order 8.
Thus the elements of orders 1,2,4 and 8 are the powers of 2, and the remaining elements are of order 16, ie they are primitive roots.
So there is 1 element of order 1, namely $1 \bmod 17$*; and there is 1 element of order 2, namely* $-1 = 16 \bmod 17$.
There are $\phi(4) = 2$ elements of order 4, namely

$$2^{\pm 2} = 4, 4^{-1} \bmod 17 = \pm 4 \bmod 17 = 4, 13 \bmod 17.$$

There are $\phi(8) = 4$ elements of order 8, namely

$$2^{\pm 1},\ 2^{\pm 3} = 2, -8, 8, -2 \bmod 17 = 2, 8, 9, 15 \bmod 17.$$

The remaining $\phi(16) - 8$ elements, namely

$$3, 5, 6, 7, 10, 11, 12, 14 \bmod 17$$

are of order 16.
[Note that

$$2 \cdot 3^2 \equiv 1 \bmod 17.$$

Hence

$$3^2 \equiv 2^{-1} \bmod 17.$$

Since 2^{-1} is of order 8, like 2, it follows that 3 is of order 16.]

5. State and prove Gauss' Law of Quadratic Reciprocity.

Does there exist an integer x such that

$$x^2 \equiv 17 \bmod 30?$$

If there is, find the least such integer ≥ 0.

Answer:

(a) If p is a prime, and $a \in \mathbb{Z}$ is coprime to p, we set

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if there is an } x \in \mathbb{Z} \text{ such that } a \equiv x^2 \bmod p, \\ -1 & \text{if there is no such } x. \end{cases}$$

Theorem. If p, q are distinct odd primes then

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

(b) There are many proofs of the Quadratic Reciprocity Theorem. Here is Zolotarev's proof, based on the parity (even or odd) of a permutation.

Recall that a permutation $\pi \in S_n$ is even or odd according as it transforms the alternating polynomial

$$A = \prod_{i<j}(x_i - x_j)$$

into $\pm A$. We set

$$\epsilon(\pi) = \begin{cases} +1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd.} \end{cases}$$

Evidently the map

$$\pi \to \epsilon(\pi) : (\mathbb{Z}/p)^* \to \{\pm 1\}$$

is a homomorphism.

We know that every permutation π can be expressed as a product of transpositions. It is easy to see that π is even or odd according as the number of transpositions is even or odd. Also, an even cycle is odd, and an odd cycle is even.

Lemma. Suppose p is an odd prime, and a is coprime to p. Let π denote the permutation

$$x \to ax \bmod p : (\mathbb{Z}/p)^* \to (\mathbb{Z}/p)^*.$$

Then

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

Proof. Recall Eisenstein's Criterion:

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

It follows that $\left(\frac{a}{p}\right) = \pm 1$ according as the order of $a \bmod p$ does or does not divide $(p-1)/2$.
Suppose the order of a is d. Then the permutation π divides into $(p-1)/d$ cycles of length d.
If $d \mid (p-1)/2$ then $(p-1)/d$ is even, and so $\epsilon(\pi) = 1$.
If $d \nmid (p-1)/2$ then $(p-1)/d$ is odd, and d is even, and so $\epsilon(\pi) = -1$. □

Let us arrange the elements $0, 1, 2, \ldots, pq-1$. *in the form of a* $p \times q$ *matrix:*

$$\begin{pmatrix} 0 & 1 & \cdots & q-1 \\ q & q+1 & \cdots & 2q-1 \\ \cdots & \cdots & \cdots & \cdots \\ (p-1)q & (p-1)q+1 & \cdots & pq-1 \end{pmatrix}$$

Thus the matrix contains the element $qj+i$ *in position* (i,j).
For each $r \in [0, pq)$ *let* $\mu(r)$ *denote the remainder of* $r \bmod q$, *ie*

$$\mu(r) \equiv r \bmod q \qquad (0 \le \mu(r) < q).$$

Now let us permute each row in the above matrix, sending

$$qj + i \to qj + \mu(pi).$$

Thus the matrix becomes

$$\begin{pmatrix} 0 & p' & \cdots & q-p' \\ q & q+p' & \cdots & 2q-p' \\ \cdots & \cdots & \cdots & \cdots \\ (p-1)q & (p-1)q+p' & \cdots & pq-p' \end{pmatrix},$$

where $p' = \mu(p)$
Each row has been permuted in the same way, and we have seen above that the signature of this permutation is $\left(\frac{p}{q}\right)$. *Since there are an odd number of rows, it follows that the permutation of the matrix elements has signature*

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

Notice that each column in the permuted matrix above appears in correct cyclic order, ie if the first element in the ith column is $i' = \mu(pi)$ then the subsequent elements are $q+i',\ 2q+i', \ldots, (p-1)q+i'$. Since one of these elements is pi, we can perform a cyclic permutation of the column to bring the elements to $pi,\ q+pi,\ 2q+pi, \ldots, (p-1)q+pi$ (where we are taking all elements $\mathrm{mod} pq$*).*
As there are an odd number of elements in each column, each of these cyclic permutations will be even. So the new permutation

$$\Pi : \begin{pmatrix} 0 & 1 & \cdots & q-1 \\ q & q+1 & \cdots & 2q-1 \\ \cdots & \cdots & \cdots & \cdots \\ (p-1)q & (p-1)q+1 & \cdots & pq-1 \end{pmatrix} \to \begin{pmatrix} 0 & p & 2p & \\ q & q+p & q+2p & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ (p-1)q & (p-1)q+p & (p-1)q+2p & \end{pmatrix}$$

will still have signature

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

It follows in the same way, on swapping p and q, that the permutation of the $q \times p$ matrices

$$\Pi' : \begin{pmatrix} 0 & 1 & \cdots & p-1 \\ p & p+1 & \cdots & 2p-1 \\ \cdots & \cdots & \cdots & \cdots \\ (q-1)p & (q-1)p+1 & \cdots & pq-1 \end{pmatrix} \to \begin{pmatrix} 0 & q & 2q & \\ p & p+q & p+2q & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ (q-1)p & (q-1)p+q & (q-1)p+2q & \end{pmatrix}$$

has signature

$$\epsilon(Pi') = \left(\frac{q}{p}\right).$$

Evidently the "target" matrices in the two cases are transposes of one another. So we have to determine the signature of the permutation

$$\Theta : qj + i \mapsto pi + j$$

defined by the transposition.
We know that the signature of a permutation π of $\{1, 2, \ldots, n\}$ is $(-1)^r$, where r is the number of inversions, ie the number of u, v with

$$u < v \leq n \text{ and } \pi(u) > \pi(v).$$

In our case

$$(i, j) = qi + j < (i', j') = qi' + j' \text{ if } i < i' \text{ or } i = i' \text{ and } j < j'.$$

We have to determine in these cases if

$$[i,j] = pj + i < [i',j'] = pj' + i'.$$

Thus we have to determine the number of i, j *with*

$$i < i' \text{ and } j > j'.$$

This number is

$$((p-1)+(p-2)+\cdots+1))\,((q-1)+(q-2)+\cdots+q)) = p(p-1)/2 \cdot q(q-1)/2.$$

Since p, q *are odd, it follows that*

$$\epsilon(\Theta) = (-1)^{(p-1)/2\cdot(q-1)/2}.$$

Since

$$\Pi' = \Pi\Theta,$$

the result follows:

$$\epsilon(\Pi') = \epsilon(\Pi)\epsilon(\Theta),$$

ie

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

ie

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

(c) *By the Chinese Remainder Theorem there will exist such an integer if each of the congruences*

$$x^2 \equiv 17 \bmod 2,$$
$$y^2 \equiv 17 \bmod 3,$$
$$z^2 \equiv 17 \bmod 5,$$

is soluble. The second is not soluble, since

$$17 \equiv 2 \bmod 3,$$

and

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

Hence the given congruence is not soluble.

6. Prove that the ring Γ of gaussian integers $m + ni$ is a Unique Factorisation Domain, and determine the units and primes in this domain.

   Show that an integer $n > 0$ can be expressed in the form

$$n = a^2 + b^2 \quad (a, b \in \mathbb{N})$$

   if and only if each prime $p \equiv 3 \bmod 4$ divides n to an even power.

   In how many ways can 1 million be expressed as a sum of two squares?

   Answer:

   (a) If $z = x + yi$, where $x, y \in \mathbb{R}$, we set $\bar{z} = x - yi$, and

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

   It is readily established that

   i. $\mathcal{N}(z) \in \mathbb{Q}$;
   ii. $\mathcal{N}(z) \geq 0$ *and* $\mathcal{N}(z) = 0 \iff z = 0$;
   iii. If $z \in \Gamma$ *then* $\mathcal{N}(z) \in \mathbb{N}$.
   iv. $\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w)$;
   v. If $a \in \mathbb{Q}$ *then* $\mathcal{N}(a) = a^2$;

   Lemma. Suppose $z, w \in \Gamma$, with $w \neq 0$. Then we can find $q, r \in \Gamma$ such that

$$z = qw + r,$$

   with

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

   Proof. Suppose

$$\frac{z}{w} = x + iy,$$

   where $x, y \in \mathbb{Q}$.

   Let $m, n \in \mathbb{Z}$ be the nearest integers to x, y, respectively. Then

$$|x - m| \leq \frac{1}{2},\ |y - n| \leq \frac{1}{2}.$$

   Set

$$q = m + in.$$

   Then

$$\frac{z}{w} - q = (x - m) + i(y - n).$$

Thus

$$\mathcal{N}(\frac{z}{w} - 1) = (x - m)^2 + (y - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

But

$$\begin{aligned}\mathcal{N}(\frac{z}{w} - 1) &= \mathcal{N}(\frac{z - qw}{w}) \\ &= \frac{\mathcal{N}(z - qw)}{\mathcal{N}(w)}.\end{aligned}$$

Hence

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

from which the result follows on setting

$$r = z - qw.$$

□

Lemma. Any two numbers $z, w \in \Gamma$ have a greatest common divisor δ such that

$$\delta \mid z, w$$

and

$$\delta' \mid z, w \implies \delta' \mid \delta.$$

Also, δ is uniquely defined up to multiplication by a unit.
Moreover, there exists $u, v \in \Gamma$ such that

$$uz + vw = \delta.$$

Proof. We follow the classic Euclidean Algorithm, except that we use $\mathcal{N}(z)$ in place of $|n|$.
We start by dividing z by w:

$$z = q_0 w + r_0, \quad \mathcal{N}(r_0) < \mathcal{N}(w).$$

If $r_0 = 0$, we are done. Otherwise we divide w by r_0:

$$w = q_1 r_0 + r_1, \quad \mathcal{N}(r_1) < \mathcal{N}(r_0).$$

f $r_1 = 0$, we are done. Otherwise we continue in this way. Since

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

and the norms are all positive integers, the algorithm must end, say

$$r_i = q_i r_{i-1},\ r_{i+1} = 0.$$

Setting

$$\delta = r_i,$$

we see successively that

$$\delta \mid r_{i-1}, r_{i-2}, \ldots, r_0, w, z.$$

Conversely, if $\delta' \mid z, w$ then

$$\delta' \mid z, w, r_0, r_1, \ldots, r_i = \delta.$$

The last part of the Lemma follows as in the classic Euclidean Algorithm; we see successively that $r_1, r_2, \ldots, r_i = \delta$ are each expressible as linear combinations of z, w with coefficients in Γ. $\square$

Theorem. Γ is a Unique Factorisation Domain.

Proof. First we show that any $z \in \Gamma$ is a product of irreducibles, by induction on $\mathcal{N}(z)$.
If z is a unit or irreducible, we are done. If not, suppose

$$z = wt,$$

where neither w nor t is a unit. Then

$$\mathcal{N}(z) = \mathcal{N}(w)\mathcal{N}(t) \implies \mathcal{N}(w), \mathcal{N}(t) < \mathcal{N}(z).$$

Hence w, t are products of prime elements, and the result follows.
To see that the expression is unique, we must establish the analogue of Euclid's Lemma. The proof is identical to the classic case.

Lemma. *If $\pi \in \Gamma$ is prime element and $z, w \in \Gamma$ then*

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

Proof. If $\pi \nmid z$ then

$$\gcd(\pi, z) = 1.$$

Hence there exist u, v such that

$$u\pi + vz = 1.$$

Multiplying by w, Multiplying by w,

$$u\pi w + vzw = w.$$

Since π divides both terms on the left,

$$\pi \mid w.$$

□

Now the proof is as before. Again, we argue by induction on $\mathcal{N}(z)$. Suppose

$$z = \epsilon p_1 \cdots p_r = \epsilon' p_1' \ldots p_s'.$$

Then

$$\pi_1 \mid \pi_i'$$

for some i. Hence

$$\pi_i' \sim \pi.$$

Now we can divide both sides by π_1 and apply the inductive hypothesis. □

(b) **Lemma.** $e \in \Gamma$ is a unit if and only if $\mathcal{N}(e) = 1$.

Proof. If e is a unit, ie $ef = 1$ for some $f \in \Gamma$, then

$$\mathcal{N}(ef) = 1 \implies \mathcal{N}(e) = \mathcal{N}(f) = 1.$$

Conversely, if $\mathcal{N}(e) = 1$ then $e\bar{e} = 1$, and so e is a unit, since $\bar{e} \in \Gamma$. □

It follows that $e = m + ni$ is a unit if and only if

$$m^2 + n^2 = 1.$$

Evidently the only solutions to this are $(m, n) = (\pm 1, 0), (0, \pm 1)$. Thus the only units in Γ are $\pm 1, \pm i$.

(c) **Lemma.** An odd prime $p \in \mathbb{N}$ splits in Γ if and only if $p \equiv 1 \bmod 4$.

Proof. Suppose p splits, say

$$p = \pi_1 \cdots \pi_r.$$

Then

$$p^2 = \mathcal{N}(p) = \mathcal{N}(p_1) \cdots \mathcal{N}(pi_r).$$

It follows (from prime factorization in $\mathbb{N}$) that $r = 2$ and

$$\mathcal{N}(\pi_1) = \mathcal{N}(\pi_2) = p.$$

Let $\pi = \pi_1 = m + ni$. Then

$$\mathcal{N}(\pi) = m^2 + n^2 = p.$$

Clearly n is coprime to p. So if n^{-1} denotes the inverse of n modulo p then

$$(mn^{-1})^2 + 1 \equiv 0 \bmod p.$$

Hence -1 is a quadratic residue modulo p. But we know (from Euler's Criterion) that this holds if and only if $p \equiv 1 \bmod 4$. So p remains prime in Γ if $p \equiv 3 \bmod 4$.
Suppose $p \equiv 1 \bmod 4$. Then there is an r such that

$$r^2 + 1 \equiv 0 \bmod p,$$

ie

$$(r + i)(r - i) = pm.$$

If p does not split then

$$p \mid r \pm i \implies p \mid 1,$$

which is absurd. □

Finally,

$$2 = i(1 - i)^2.$$

Thus 2 ramifies in Γ*, ie splits into two equal primes.*
These give all the primes in Γ*; for if* π *is a prime and*

$$\mathcal{N}(\pi) = n = p_1 \cdots p_r$$

then $\pi \mid p_i$ *for some* i*.*

(d) Suppose

$$n = a^2 + b^2,$$

and suppose $p \equiv 3 \bmod 4$ *divides* n*. Then it follows from the argument above that* $p \mid a, b$*; for otherwise* -1 *would be a quadratic residue modulo* p*. Thus* $p^2 \mid n$*, and*

$$n/p^2 = (a/p)^2 + (b/p)^2.$$

We deduce, on repeating this argument, that p divides n to an even power.

Now suppose

$$n = 2^e p_1^{e_1} \cdots p_r^{e_r} q_1^{2f_1} \cdots q_s^{2f_s},$$

where $p_i \equiv 1 \bmod 4,\ q_j \equiv 3 \bmod 4$. *If now*

$$p_i = \pi_i \bar{\pi}_i.$$

set

$$z = a + ib = (1-i)^e \pi_1^{e_1} \cdots \pi_r^{e_r} q_1^{f_1} \cdots q_s^{f_r}.$$

Then

$$\mathcal{N}(z) = a^2 + b^2 = n.$$

(e) Suppose

$$1000000 = 2^6 5^6 = a^2 + b^2.$$

We shall assume that $a, b \geq 0$, *and that* $a \geq b$. *By the above argument*

$$a + ib = f(1-i)^6 (2+i)^s (2-i)^t,$$

where f is a unit and $r + s = 6$. The unit f is uniquely defined by the conditions $a, b \geq 0,\ a \geq b$, *Hence there are 7 different ways of expressing 10000000 as a sum of two squares.*

7. Define an *algebraic number* and an *algebraic integer*.

Show that the algebraic numbers form a field, and the algebraic integers form a commutative ring.

Prove that $(\sqrt{2} + \sqrt{3})/2$ is not an algebraic integer.

Answer:

(a) We say that $\alpha \in \mathbb{C}$ is an algebraic number if it satisfies an equation

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

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

(b) We say that α is an algebraic integer if it satisfies an equation

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

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

(c) **Lemma.** Suppose

$$\alpha V \subset V,$$

where $V \subset \mathbb{C}$ is a finite-dimensional vector space. Then α is an algebraic number.

Proof. Let $e_1, \ldots, e_n$ be a basis for V. Then

$$\begin{aligned}
\alpha e_1 &= a_{11}e_1 + \cdots + a_{1n}e_n, \\
\alpha e_2 &= a_{21}e_1 + \cdots + a_{2n}e_n, \\
&\cdots \\
\alpha e_n &= a_{11}e_1 + \cdots + a_{1n}e_n,
\end{aligned}$$

where $a_{ij} \in \mathbb{Q}$.
It follows that α satisfies the polynomial equation

$$\det(xI - A) = 0.$$

This has rational coefficients. Hence α is algebraic. □

Now suppose α, β are algebraic, satisfying the equations

$$\begin{aligned}
x^m + a_1 x^{m-1} + \cdots + a_m = 0, \\
x^n + b_1 x^{n-1} + \cdots + b_n = 0.
\end{aligned}$$

Consider the vector subspace $V \subset \mathbb{C}$ over $\mathbb{Q}$ spanned by the mn numbers

$$\alpha^i \beta^j \qquad (1 \leq i \leq m,\ 1 \leq j \leq n).$$

It is readily verified that

$$\alpha V \subset V,\ \beta V \subset V.$$

It follows that

$$(\alpha + \beta)V \subset V,\ (\alpha\beta)V \subset V.$$

Hence $\alpha + \beta,\ \alpha\beta$ are algebraic.
Since it is easy to see that α^{-1} is algebraic, it follows that the algebraic numbers form a field.

(d) **Lemma.** Suppose

$$\alpha A \subset A,$$

where $A \subset \mathbb{C}$ is a finitely-generated abelian group Then α is an algebraic integer.

Proof. This follows in the same way as the last Lemma, with α satisfying an equation

$$\det(xI - A) = 0,$$

where now the coefficients are integers. □

(e) *Suppose*

$$\alpha = (\sqrt{2} + \sqrt{3})/2$$

is an algebraic integer.
We know that $\sqrt{2}$ *and* $\sqrt{3}$ *are algebraic integers. Hence so is*

$$\sqrt{2} - \sqrt{3};$$

and so therefore is

$$\alpha(\sqrt{2} - \sqrt{3}) = -\frac{1}{2}.$$

Suppose $-1/2$ *satisfies the equation*

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

with $a_1, \ldots, a_n \in \mathbb{Z}$. *Multiplying by* 2^n,

$$1 + 2a_1 + 4a_2 + \cdots + 2^n a_n = 0 \implies 2 \mid 1.$$

8. Show that the ring $\mathbb{Z}[\sqrt{3}]$ formed by the numbers $m + n\sqrt{3}$ $(m, n \in \mathbb{Z})$ is a Unique Factorisation Domain.

   Determine the units and primes in this domain.

   Is $\mathbb{Z}[\sqrt{6}]$ a Unique Factorisation Domain?

   Answer:

   (a) *Let*

   $$A = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}.$$

   The numbers $\{x + y\sqrt{3} : x, y \in \mathbb{Q}\}$ *form a field* $\mathbb{Q}(\sqrt{3})$. *(Recall that A is the ring of algebraic integers in this field.) If* $z = x + y\sqrt{3}$ *we set*

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

   and

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

   Lemma. Given $z, w \in A$ with $w \neq 0$ we can find $q, r \in A$ such that

   $$z = qw + r$$

   with

   $$|\mathcal{N}(()r)| < |\mathcal{N}(()q)|\,.$$

Proof. Let

$$\frac{z}{w} = x + y\sqrt{3},$$

with $x, y \in \mathbb{Q}$. We can find $m, n \in \mathbb{Z}$ such that

$$|x - m| \leq \frac{1}{2},\ |y - n| \leq \frac{1}{2}.$$

Choose

$$q = m + ni.$$

Then

$$-\frac{3}{4} \leq \mathcal{N}(()\frac{z}{w} - q) \leq \frac{1}{4}.$$

It follows from the multiplicative property of the norm that

$$|\mathcal{N}(()z - qw)| \leq \frac{3}{4}\,|\mathcal{N}(q)|\,,$$

and the result follows on setting $r = z - qw$. □

This Lemma allows us to set up the Euclidean Algorithm in A, and so define

$$\gcd(z, w) = \delta$$

for $z, winA$.
Moreover, it follows by reversing the algorithm that we can find $u, v \in A$ such that

$$uz + vw = \delta.$$

The analogue of Euclid's Lemma follows: if $\pi \in \Gamma$ is irreducible then

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

Any $z \in \Gamma$ can be expressed as a product of irreducibles. For

$$z = w_1 w_2 \cdots w_r \implies \mathcal{N}(()z) = \mathcal{N}(()w_1)\mathcal{N}(()w_2)\cdots\mathcal{N}(()w_r),$$

so the number of w_i in such a product is limited by the number of factors of $\mathcal{N}(()z)$.
Finally, the uniqueness of the factorisation into irreducibles (up to order) follows in the familiar way from Euclid's Lemma.

(b) *It is easy to see that $z = m + n\sqrt{3}$ is a unit in A if and only if*

$$\mathcal{N}(()z) = \pm 1.$$

For

$$zw = 1 \implies \mathcal{N}(()z)\mathcal{N}(()w) = \mathcal{N}(()1) = 1 \implies \mathcal{N}(()z) = \mathcal{N}(()w) = \pm 1.$$

Evidently

$$\epsilon = 2 + \sqrt{3}$$

is a unit, since $2^2 - 3 = 1$.

It follows that

$$\pm\epsilon^n$$

are units, for all $n \in \mathbb{Z}$.

These are in fact the only units. For suppose η *is a unit* $\neq 1$. *We may assume that*

$$\eta > 1,$$

since just one of

$$\pm\eta, \pm\eta^{-1} \in (0, \infty).$$

Suppose

$$\epsilon^n \leq \eta < \epsilon^{n+1}.$$

Then

$$\theta = \eta\epsilon^{-n} \in [1, \eta).$$

Suppose

$$\theta = m + n\sqrt{3},$$

where $m, n \in \mathbb{Z}$. *Then*

$$m - n\sqrt{3} = \pm\theta^{-1}.$$

Thus

$$1 \leq m + n\sqrt{3} < 2 + \sqrt{3},$$
$$-1 \leq m - n\sqrt{3} \leq 1.$$

Adding,

$$0 \leq m < (1 + \sqrt{3})/2.$$

Thus

$$m = 0 \text{ or } 1.$$

Since

$$m^2 - 3n^2 = \pm 1$$

it follows that

$$m = 1,\ n = 0 \implies \theta = 1.$$

(c) *Having established unique factorisation in A we may refer to irreducibles as primes.*

Suppose $p \in \mathbb{Z}$ is a rational prime. Then p factorizes into at most 2 primes in A, since

$$p = \pi_1 \cdots \pi_r \implies \mathcal{N}(()\pi_1) \cdots \mathcal{N}(()\pi_r) = \mathcal{N}(()p) = p^2,$$

and $|\mathcal{N}(()\pi_i)| > 1$ since $|\mathcal{N}(()z)| = 1$ implies that z is a unit.

Conversely, each prime $\pi \in A$ is a factor of a unique rational prime p. For if

$$\mathcal{N}(()\pi) = \pi\overline{\pi} = p_1 \cdots p_r$$

then π divides one of the p_i; and it cannot divide two different rational primes p, q since we can find $x, y \in \mathbb{Z}$ such that

$$px + qy = 1,$$

and so

$$\pi \mid p, q \implies \pi \mid 1,$$

which is absurd.

Also, if a rational prime p splits in Γ then

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

ie p splits into conjugate primes. For

$$\begin{aligned} p = \pi\pi' &\implies \mathcal{N}(()\pi)\mathcal{N}(()\pi') = Norm(p) = p^2 \\ &\implies \mathcal{N}(()\pi) = \pi\overline{\pi} = \pm p. \end{aligned}$$

Thus we have to determine which rational primes $p \in \mathbb{N}$ split in A.

Theorem.

i. 3 ramifies (ie splits into two equal primes) in A:

$$3 = (\sqrt{3})^2.$$

ii.

Lemma. Suppose $p \in \mathbb{N}$ is a rational prime. Then we can find $x \in \mathbb{Z}$ such that

$$x^2 \equiv 3 \bmod p$$

if and only if either $p = 2$ or 3, or

$$p \equiv \pm 1 \bmod 12.$$

Proof. The result is trivial if $p = 2$ or 3. If $p \neq 2, 3$, then by Gauss' Quadratic Reciprocity Law,

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

and

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

□

Suppose p is a rational prime. If $p \equiv 3 \bmod 4$ then p cannot split in Γ. For if p splits then $p = \mathcal{N}(()\pi)$ from above; but if $\pi = m+ni$ then

$$p = \mathcal{N}(()\pi) = m^2 + n^2,$$

and this is impossible if $p \equiv 3 \bmod 4$ since $m^2, n^2 \equiv 0$ or $1 \bmod 4$.
On the other hand, if $p \equiv 1 \bmod 4$ then it does split. For we know in this case that

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

ie we can find $n \in \mathbb{Z}$ such that

$$p \mid n^2 + 1.$$

But

$$n^2 + 1 = (n + i)(n - i)$$

in Γ. Thus if p remained prime in Γ we would have

$$p \mid n + i \text{ or } p \mid n - i,$$

both of which are impossible.
Finally,

$$2 = -i(1 + i)^2.$$

Thus 2 ramifies in Γ, ie splits into 2 equal (or associated) primes.

(d) **Lemma.** The integer $n \in \mathbb{N}$ is expressible as a sum of squares if and only if each prime factor $p \equiv 3 \bmod 4$ occurs to an even power in n
Thus

$$99 = 3^2 \cdot 11$$

is not expressible as a sum of 2 squares, since $11 \equiv 3 \bmod 4$ *and this occurs only once.*

Similarly

$$999 = 3^3 \cdot 37$$

is not expressible as a sum of 2 squares, since 3 occurs 3 times.

Again, 2010 is divisible by 3 but not by 9, and so is not expressible as a sum of 2 squares.

Finally, $2317 = 7 \cdot 331$ *is not expressible as a sum of 2 squares, since 7 occurs only once. (Note that it is not necessary to know that 331 is prime; it is sufficient to observe that it is not divisible by 7.)*