where $q_2' = uq_2$ is again an irreducible (associate to q_2). By induction on n, we conclude that each of the factors on the left matches bijectively (up to associates) with the factors on the far right, hence with the factors in the middle (which are the same, up to associates). Since p_1 and q_1 (after the initial renumbering) have already been shown to be associate, this completes the induction step and the proof of the theorem.

Corollary 15. *(Fundamental Theorem of Arithmetic)* The integers $\mathbb{Z}$ are a Unique Factorization Domain.

Proof: The integers $\mathbb{Z}$ are a Euclidean Domain, hence are a Unique Factorization Domain by the theorem.

We can now complete the equivalence (Proposition 9) between the existence of a Dedekind–Hasse norm on the integral domain R and whether R is a P.I.D.

Corollary 16. Let R be a P.I.D. Then there exists a multiplicative Dedekind–Hasse norm on R.

Proof: If R is a P.I.D. then R is a U.F.D. Define the norm N by setting $N(0) = 0$, $N(u) = 1$ if u is a unit, and $N(a) = 2^n$ if $a = p_1 p_2 \cdots p_n$ where the p_i are irreducibles in R (well defined since the number of irreducible factors of a is unique). Clearly $N(ab) = N(a)N(b)$ so N is positive and multiplicative. To show that N is a Dedekind–Hasse norm, suppose that a, b are nonzero elements of R. Then the ideal generated by a and b is principal by assumption, say $(a, b) = (r)$. If a is not contained in the ideal (b) then also r is not contained in (b), i.e., r is not divisible by b. Since $b = xr$ for some $x \in R$, it follows that x is not a unit in R and so $N(b) = N(x)N(r) > N(r)$. Hence (a, b) contains a nonzero element with norm strictly smaller than the norm of b, completing the proof.

Factorization in the Gaussian Integers

We end our discussion of Unique Factorization Domains by describing the irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ and the corresponding application to a famous theorem of Fermat in elementary number theory. This is particularly appropriate since the classical study of $\mathbb{Z}[i]$ initiated the algebraic study of rings.

In general, let $\mathcal{O}$ be a quadratic integer ring and let N be the associated field norm introduced in Section 7.1. Suppose $\alpha \in \mathcal{O}$ is an element whose norm is a prime p in $\mathbb{Z}$. If $\alpha = \beta\gamma$ for some $\beta, \gamma \in \mathcal{O}$ then $p = N(\alpha) = N(\beta)N(\gamma)$ so that one of $N(\beta)$ or $N(\gamma)$ is ± 1 and the other is $\pm p$. Since we have seen that an element of $\mathcal{O}$ has norm ± 1 if and only if it is a unit in $\mathcal{O}$, one of the factors of α is a unit. It follows that

if $N(\alpha)$ is $\pm$ a prime (in $\mathbb{Z}$), then α is irreducible in $\mathcal{O}$.

Suppose that π is a prime element in $\mathcal{O}$ and let (π) be the ideal generated by π in $\mathcal{O}$. Since (π) is a prime ideal in $\mathcal{O}$ it is easy to check that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ (if a and b are integers with $ab \in (\pi)$ then either a or b is an element of (π), so a or b is in $(\pi) \cap \mathbb{Z}$). Since $N(\pi)$ is a nonzero integer in (π) we have $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some integer prime p. It follows from $p \in (\pi)$ that π is a divisor in $\mathcal{O}$ of the

integer prime p, and so the prime elements in $\mathcal{O}$ can be found by determining how the primes in $\mathbb{Z}$ factor in the larger ring $\mathcal{O}$. Suppose π divides the prime p in $\mathcal{O}$, say $p = \pi\pi'$. Then $N(\pi)N(\pi') = N(p) = p^2$, so since π is not a unit there are only two possibilities: either $N(\pi) = \pm p^2$ or $N(\pi) = \pm p$. In the former case $N(\pi') = \pm 1$, hence π' is a unit and $p = \pi$ (up to associates) is irreducible in $\mathbb{Z}[i]$. In the latter case $N(\pi) = N(\pi') = \pm p$, hence π' is also irreducible and $p = \pi\pi'$ is the product of precisely two irreducibles.

Consider now the special case $D = -1$ of the Gaussian integers $\mathbb{Z}[i]$. We have seen that the units in $\mathbb{Z}[i]$ are the elements ± 1 and $\pm i$. We proved in Section 1 that $\mathbb{Z}[i]$ is a Euclidean Domain, hence is also a Principal Ideal Domain and a Unique Factorization Domain, so the irreducible elements are the same as the prime elements, and can be determined by seeing how the primes in $\mathbb{Z}$ factor in the larger ring $\mathbb{Z}[i]$.

In this case $\alpha = a + bi$ has $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$, where $\overline{\alpha} = a - bi$ is the complex conjugate of α. It follows by what we just saw that *p factors in $\mathbb{Z}[i]$ into precisely two irreducibles if and only if $p = a^2 + b^2$ is the sum of two integer squares (otherwise p remains irreducible in $\mathbb{Z}[i]$).* If $p = a^2 + b^2$ then the corresponding irreducible elements in $\mathbb{Z}[i]$ are $a \pm bi$.

Clearly $2 = 1^2 + 1^2$ is the sum of two squares, giving the factorization $2 = (1+i)(1-i) = -i(1+i)^2$. The irreducibles $1+i$ and $1-i = -i(1+i)$ are associates and it is easy to check that this is the only situation in which conjugate irreducibles $a + bi$ and $a - bi$ can be associates.

Since the square of any integer is congruent to either 0 or 1 modulo 4, an odd prime in $\mathbb{Z}$ that is the sum of two squares must be congruent to 1 modulo 4. Thus if p is a prime of $\mathbb{Z}$ with $p \equiv 3 \bmod 4$ then p is not the sum of two squares and p remains irreducible in $\mathbb{Z}[i]$.

Suppose now that p is a prime of $\mathbb{Z}$ with $p \equiv 1 \bmod 4$. We shall prove that p cannot be irreducible in $\mathbb{Z}[i]$ which will show that $p = (a + bi)(a - bi)$ factors as the product of two distinct irreducibles in $\mathbb{Z}[i]$ or, equivalently, that $p = a^2 + b^2$ is the sum of two squares. We first prove the following result from elementary number theory:

Lemma 17. The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to 1 modulo 4.

Proof: The statement for $p = 2$ is trivial since $2 \mid 1^2 + 1$. If p is an odd prime, note that $p \mid n^2 + 1$ is equivalent to $n^2 = -1$ in $\mathbb{Z}/p\mathbb{Z}$. This in turn is equivalent to saying the residue class of n is of order 4 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus p divides an integer of the form $n^2 + 1$ if and only if $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4. By Lagrange's Theorem, if $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4 then $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ is divisible by 4, i.e., p is congruent to 1 modulo 4.

Conversely, suppose $p - 1$ is divisible by 4. We first argue that $(\mathbb{Z}/p\mathbb{Z})^\times$ contains a unique element of order 2. If $m^2 \equiv 1 \bmod p$ then p divides $m^2 - 1 = (m-1)(m+1)$. Thus p divides either $m - 1$ (i.e., $m \equiv 1 \bmod p$) or $m + 1$ (i.e., $m \equiv -1 \bmod p$), so -1 is the unique residue class of order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. Now the abelian group $(\mathbb{Z}/p\mathbb{Z})^\times$ contains a subgroup H of order 4 (for example, the quotient by the subgroup $\{\pm 1\}$ contains a subgroup of order 2 whose preimage is a subgroup of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$).

Since the Klein 4-group has three elements of order 2 whereas $(\mathbb{Z}/p\mathbb{Z})^\times$ — hence also H — has a unique element of order 2, H must be the cyclic group of order 4. Thus $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4, namely a generator for H.

Remark: We shall prove later (Corollary 19 in Section 9.5) that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group, from which it is immediate that there is an element of order 4 if and only if $p-1$ is divisible by 4.

By Lemma 17, if $p \equiv 1 \bmod 4$ is a prime then p divides n^2+1 in $\mathbb{Z}$ for some $n \in \mathbb{Z}$, so certainly p divides $n^2+1 = (n+i)(n-i)$ in $\mathbb{Z}[i]$. If p were irreducible in $\mathbb{Z}[i]$ then p would divide either $n+i$ or $n-i$ in $\mathbb{Z}[i]$. In this situation, since p is a real number, it would follow that p divides both $n+i$ and its complex conjugate $n-i$; hence p would divide their difference, $2i$. This is clearly not the case. We have proved the following result:

Proposition 18.

(1) *(Fermat's Theorem on sums of squares)* The prime p is the sum of two integer squares, $p = a^2+b^2$, $a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \bmod 4$. Except for interchanging a and b or changing the signs of a and b, the representation of p as a sum of two squares is unique.

(2) The irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows:

- **(a)** $1+i$ (which has norm 2),
- **(b)** the primes $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$ (which have norm p^2), and
- **(c)** $a+bi$, $a-bi$, the distinct irreducible factors of $p = a^2+b^2 = (a+bi)(a-bi)$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \bmod 4$ (both of which have norm p).

The first part of Proposition 18 is a famous theorem of Fermat in elementary number theory, for which a number of alternate proofs can be given.

More generally, the question of whether the integer $n \in \mathbb{Z}$ can be written as a sum of two integer squares, $n = A^2+B^2$, is equivalent to the question of whether n is the norm of an element $A+Bi$ in the Gaussian integers, i.e., $n = A^2+B^2 = N(A+Bi)$. Writing $A+Bi = \pi_1\pi_2\cdots\pi_k$ as a product of irreducibles (uniquely up to units) it follows from the explicit description of the irreducibles in $\mathbb{Z}[i]$ in Proposition 18 that n is a norm if and only if the prime divisors of n that are congruent to 3 mod 4 occur to even exponents. Further, if this condition on n is satisfied, then the uniqueness of the factorization of $A+Bi$ in $\mathbb{Z}[i]$ allows us to count the number of representations of n as a sum of two squares, as in the following corollary.

Corollary 19. Let n be a positive integer and write

$$n = 2^k p_1^{a_1}\cdots p_r^{a_r} q_1^{b_1}\cdots q_s^{b_s}$$

where $p_1, \ldots, p_r$ are distinct primes congruent to 1 modulo 4 and $q_1, \ldots, q_s$ are distinct primes congruent to 3 modulo 4. Then n can be written as a sum of two squares in $\mathbb{Z}$, i.e., $n = A^2+B^2$ with $A, B \in \mathbb{Z}$, if and only if each b_i is even. Further, if this condition on n is satisfied, then the number of representations of n as a sum of two squares is $4(a_1+1)(a_2+1)\cdots(a_r+1)$.