III. Two elements a, b of A are called *relatively prime* if $\gcd(a, b) = 1$. Let us recall the important LEMMA OF EUCLID. *Let a, b, c be elements in a principal ideal ring A. If a divides bc and is relatively prime to b, then a divides c.*

A quick proof of Euclid's lemma. By Bezout (2) there exist a' and $b' \in A$ such that $1 = a'a + b'b$; whence $c = a'ac + b'bc$. Since a divides both terms on the right-hand side, a divides c as well.

IV. Finally there is unique factorization into products of primes.

Theorem. Let A be a principal ideal ring and let K be its field of fractions. There exists a subset $P \subset A$ such that any $x \in K$ may be uniquely expressed in the form

$$x = u \prod_{p \in P} p^{v_p(x)}, \tag{6}$$

where u is a unit in A and where the exponents $v_p(x)$ are elements of $\mathbf{Z}$, all zero except for a finite subset among them.

For a more systematic exposition of these topics we refer the reader to [1]. *Algèbre*, Chapter VI, § 1 and Chapter VII, § 1. Part of the theory (more precisely everything which doesn't depend upon Bezout's identity) extends to more general rings than principal ideal rings. We are referring to *unique factorization domains* or *factorial rings* See [1] or [2] *Algèbre commutative*, Chapter VII, § 3.

1.2 An example: the diophantine equations $X^2 + Y^2 = Z^2$ and $X^4 + Y^4 = Z^4$.

One of the most attractive parts of number theory is the study of *diophantine equations* One considers polynomial equations $P(X_1, \ldots, X_n) = 0$ with coefficients in $\mathbf{Z}$ (respectively, in $\mathbf{Q}$) and one seeks solutions (x_i) in $\mathbf{Z}$ (respectively, in $\mathbf{Q}$). One can replace $\mathbf{Z}$ (respectively, $\mathbf{Q}$) by more general rings A (respectively, fields K). We will give an example later (§ 6).

We are going to study here two special cases of Fermat's famous equation:

$$X^n + Y^n = Z^n. \tag{1}$$

Fermat claimed to have shown that, for $n \geq 3$, this equation has no non-trivial integer solution (x, y, z). His proof has never been found. Numerous mathematicians have since Fermat's time worked intensively on this problem. They have shown that Fermat's claim is true for a great many values of the exponent n. Nevertheless, no general proof (i.e. valid for any n) has been found.

Present-day opinion holds that, in his "proof", Fermat made a mistake, but a mistake worthy of a first-class mathematician. For example he might have conceived the idea (ingenious for his time) of working in the ring of integers of a field containing nth roots of unity; he may have believed that such a ring is always a principal ideal ring. In fact, we know how to prove Fermat's claim for any exponent n for which the ring of nth roots of unity is a principal ideal ring. However, this is not the case for all n. For n prime, this ring is a principal ideal ring only for finitely many values of n.[1]

For $n = 2$, equation (1) has integer solutions, e.g. (3, 4, 5). One can give a complete description of all the integer solutions of (1).

1. Cf. C. L. Siegel "Gesammelte Werke", Part III, pp. 436–442.

Theorem 1. If x, y, z are positive integers such that $x^2 + y^2 = z^2$, then there exists an integer d and two relatively prime integers u and v such that (except, possibly, for a permutation of x and y):

$$x = d(u^2 - v^2), \quad y = 2duv, \quad \text{and} \quad z = d(u^2 + v^2). \tag{2}$$

Proof. An easy calculation shows that formula (2) gives solutions for $X^2 + Y^2 = Z^2$. Conversely, let x, y, and z be positive integers such that $x^2 + y^2 = z^2$. After dividing x, y, z by their greatest common divisor, we may assume that the three numbers are relatively prime. It follows that they are pairwise relatively prime as well; for example, if x and z have a common prime factor p, then p divides $y^2 = z^2 - x^2$ and, therefore, also y. In particular, two of the numbers x, y, z are odd; the third is necessarily even. The numbers x and y cannot both be odd, for, if they were, we would have $x^2 \equiv 1 \pmod 4$, $y^2 \equiv 1 \pmod 4$, and $z^2 \equiv 2 \pmod 4$, which contradicts the fact that z^2 is a square. We have, then, after possibly switching x and y:

$$x \text{ odd}, y \text{ even, and } z \text{ odd}. \tag{3}$$

Note that

$$y^2 = z^2 - x^2 = (z - x)(z + x). \tag{4}$$

Since the greatest common divisor of $2x$ and $2z$ is 2, and since $2x = (z + x) - (z - x)$, $2z = (z + x) + (z - x)$, the greatest common divisor of $z - x$ and $z + x$ can only be 2. Put $y = 2y'$, $z + x = 2x'$, $z - x = 2z'$, where y', x', and z' are integers (since y, $z + x$, and $z - x$ are even by (3)). We have $y'^2 = x'z'$. Since x' and z' are relatively prime, we see that x' and z' are squares u^2 and v^2; in fact any prime factor of y'^2 appears, with an even exponent, either in the prime factorization of x' or in that of z', but not in both. We thus have $z + x = 2u^2$, $z - x = 2v^2$, and $y^2 = 2u^2 \cdot 2v^2$; whence, $x = u^2 - v^2$, $y = 2uv$, and $z = u^2 + v^2$. Here u and v are relatively prime, since otherwise x, y, z would have a common prime factor. Multiplying through by the greatest common divisor of x, y, z, call it d, we obtain (2). Q.E.D.

Theorem 2. The equation $X^4 + Y^4 = Z^2$ has no solution in positive integers x, y, z.

Proof. If there is a solution (x, y, z), where x, y, and z are positive integers, then there is such a solution in which z is *minimal*. In this case, x, y, and z are pairwise relatively prime; if for example x and y have a common prime factor p, then p^4 divides z^2, so p^2 divides z and $(x/p, y/p, z/p^2)$ would be a solution, contradicting the minimality of z. The two other cases are analogous and even easier. As our equation may be written as $(X^2)^2 + (Y^2)^2 = Z^2$, we may apply Theorem 1 to it. After possibly permuting x and y we see that there are positive relatively prime integers u and v such that

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad \text{and} \quad z = u^2 + v^2. \tag{5}$$

Since $4 \mid y^2$, the relation $y^2 = 2uv$ implies that one of the two numbers u and v is even; the other is necessarily odd. Thus, u even and v odd entails $u^2 \equiv 0 \pmod 4$ and $v^2 \equiv 1 \pmod 4$, whence $x^2 = u^2 - v^2 \equiv -1 \pmod 4$, an impossibility. So u is odd and $v = 2v'$. The relation $y^2 = 4uv'$ and the fact that u and v' are relatively prime implies that u and v' are squares a^2 and b^2. We apply Theorem 1 once more, this time to the

equation $x^2 + v^2 = u^2$ (cf (5)). Since x and u are odd, v even, and x, v, and u pairwise prime, we obtain two relatively prime positive integers c and d such that.

$$x = c^2 - d^2, \quad v = 2cd, \quad \text{and} \quad u = c^2 + d^2. \tag{6}$$

Now, from $v = 2v' = 2b^2$, it follows that $cd = b^2$, so that c and d are again squares x'^2 and y'^2 (they are relatively prime). Since $u = a^2$, (6) may be rewritten as

$$a^2 = x'^4 + y'^4, \tag{7}$$

which is of the same form as the original equation. On the other hand, by (5), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, whence $z > a$, which contradicts the minimality of z Theorem 2 is proved.

A slight variant of our proof shows that, given a solution (x, y, z) in positive integers of $X^4 + Y^4 = Z^2$, one may construct an infinite sequence (x_n, y_n, z_n) of such solutions, where the sequence (z_n) is strictly decreasing This is an absurdity This method of proof is called the method of infinite descent and is due to Fermat.

Corollary. The equation $X^4 + Y^4 = Z^4$ *has no positive integer solutions.*

Proof. This equation may be written in the form $X^4 + Y^4 = (Z^2)^2$, to which Theorem 2 applies.

1.3. Some lemmas concerning ideals; Euler's φ-function

Let $n \geq 1$ be a natural number. We write $\varphi(n)$ for the number of integers q, $0 \leq q \leq n$, such that q and n are relatively prime (since 0 and n are divisible by n, it is equivalent to take $1 \leq q \leq n - 1$ for any $n > 1$; set $\varphi(1) = 1$). The function φ so defined is called Euler's φ-function. If p is a prime number, then clearly:

$$\varphi(p) = p - 1. \tag{1}$$

For $n = p^s$, a power of a prime, the integers relatively prime to n are those integers which are not multiples of p. There are p^{s-1} multiples of p between 1 and p^s. Therefore,

$$\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1). \tag{2}$$

Now we intend to calculate $\varphi(n)$ by making use of the fact that n may be expressed as a product of powers of primes. For this purpose we need some properties of $\varphi(n)$ and we need some lemmas concerning ideals. These lemmas will be useful later.

Proposition 1. Let $n \geq 1$ *be a natural number. The value* $\varphi(n)$ *of Euler's* φ*-function equals the number of elements of* $\mathbf{Z}/n\mathbf{Z}$ *which generate this group. It also equals the number of units in the ring* $\mathbf{Z}/n\mathbf{Z}$.

Proof. Let us recall that each congruence class mod $n\mathbf{Z}$ contains a unique integer q such that $0 \leq q \leq n - 1$. For such an integer q we write $\bar{q}$ for its residue class mod $n\mathbf{Z}$. It suffices to prove the following implications: q relatively prime to $n \Rightarrow \bar{q}$ a unit in the ring $\mathbf{Z}/n\mathbf{Z} \Rightarrow \bar{q}$ generates the additive group $\mathbf{Z}/n\mathbf{Z} \Rightarrow q$ relatively prime to n. If q is relatively prime to n, Bezout's identity (§ **1**, (2)) implies that there are integers x and y