Which positive integers can be written as the difference of two squares, i.e. for which n is the equation $x^2 - y^2 = n$ solvable in integers? Factoring the LHS, we obtain $(x+y)(x-y) = n$, thus $x + y = d$ and $x - y = n/d$ for some $d \mid n$. This gives $x = (d + n/d)/2$ and $y = (d - n/d)/2$. We obtain integers iff either both d and n/d are odd, or both are even, which is possible iff n is odd or $4 \mid n$. It is not hard to determine the number of solutions, as well.

Now we raise the analogous question for sums instead of differences, i.e. which positive integers can be represented as the sum of two squares and in how many ways.

In solving equation $x^2 - y^2 = n$, the key step was factoring the LHS. For the case $x^2 + y^2 = n$, we have no such factorization among the integers (or even among the real numbers), but we can do it among the complex numbers: $(x + yi)(x - yi) = n$. Therefore it is promising to develop number theory for complex numbers $\alpha = a + bi$ where a and b are integers. These complex numbers are called *Gaussian integers*.

The Gaussian integers form an integral domain, i.e. a commutative ring without zero divisors and with a multiplicative identity under the addition and multiplication of complex numbers. The notions of divisibility, unit, associate, greatest common divisor, irreducible, and prime are the same as among the integers or polynomials or in any integral domain. We show that the Unique Factorization theorem (UFT) is true for the Gaussian integers, and "list" all Gaussian primes. This makes possible to handle our original problem, the Diophantine equation $x^2 + y^2 = n$.

The norm plays a central role in the number theory of Gaussian integers: $N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2$. The following simple but important features of the norm follow immediately from the definition of Gaussian integers and from the properties of the absolute values of complex numbers: $N(\alpha)$ is a non-negative integer; $N(\alpha) = 0 \iff \alpha = 0$; and $N(\alpha\beta) = N(\alpha)N(\beta)$.

The following (one-way) bridge is an important connection between integers and Gaussian integers: If $\beta \mid \alpha$ (among the Gaussian integers), then $N(\beta) \mid N(\alpha)$ (among the integers) (but the converse is false).

The units, i.e. the Gaussian integers dividing every Gaussian integer have several equivalent characterizations: (*) $\varepsilon \mid 1$; (**) $N(\varepsilon) = 1$; (***) $\varepsilon = 1, -1, i$, or $-i$.

The Gaussian integers form a Euclidean ring with the following division algorithm: To any Gaussian integers α and $\beta \neq 0$, there exist Gaussian integers γ and ϱ satisfying $\alpha = \beta\gamma + \varrho$ and $N(\varrho) < N(\beta)$.

Proof: The condition is equivalent to

$$\frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \qquad \text{and} \qquad |\varrho| < |\beta|, \quad \text{i.e.} \quad \left|\frac{\varrho}{\beta}\right| < 1.$$

Thus we have to find a Gaussian integer γ satisfying

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1\,. \tag{1}$$

The Gaussian integers form the usual unit square lattice in the complex plane. Hence, condition (1) means that the point (of rational coordinates) in the plane corresponding to α/β is closer to lattice point γ than 1, i.e. it falls inside the unit circle around γ.

Consider a unit square in the lattice which contains α/β (inside or on its border; there are more than one such unit squares iff at least one of the coordinates of α/β is an integer). If we draw unit circles around two opposite vertices, the interiors of these circles cover altogether this unit square entirely except the two other vertices. This means that to any point in the plane, there is a lattice point of distance less than 1. So to any α/β, there is a suitable γ.

The value of ϱ is determined then by $\varrho = \alpha - \beta\gamma$. ■

Remarks: 1. We see from the proof that the quotient γ and the remainder ϱ are not unique in general; uniqueness holds iff α/β itself is a lattice point, i.e. $\beta \mid \alpha$ (and the remainder is 0). Otherwise there are 2, 3, or 4 suitable pairs γ, ϱ, depending on the position of α/β.

2. The proof yields also an algorithm to find γ and ϱ: we can choose γ as (one of) the closest lattice point(s) to α/β. In a purely algebraic formulation: If $\alpha/\beta = r + si$, then choose $\gamma = u + vi$ where u and v are (one of) the closest integers to the (rational) number r and s, resp. Then

$$\left|\frac{\alpha}{\beta} - \gamma\right|^2 = (r-u)^2 + (s-v)^2 \le \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}\,.$$

Our next goal is to characterize all Gaussian primes. As a preparation, we establish a relation between Gaussian primes and "ordinary" prime numbers in $\mathbf{Z}$:

(i) To every Gaussian prime π, there exists exactly one positive prime number p satisfying $\pi \mid p$.

(ii) Every positive prime number p is either a Gaussian prime itself, or it is the product of two complex conjugate Gaussian primes having norm p.

Proof: (i) As π is different from 0 and units, we have $N(\pi) > 1$, so $N(\pi)$ is the product of positive prime numbers: $N(\pi) = p_1 p_2 \dots p_r$. Then

$$\pi \mid \pi\overline{\pi} = N(\pi) = p_1 p_2 \dots p_r,$$

and π is a Gaussian prime, thus π must divide some p_i, as well.

To prove uniqueness by contradiction, we assume $\pi \mid p$ and $\pi \mid q$ for some positive prime numbers $p \neq q$. Since p and q are coprime (among the integers), we have $1 = pu + qv$ with suitable integers u and v. Then $\pi \mid p$ and $\pi \mid q$ imply $\pi \mid pu + qv = 1$, which is a contradiction.

(ii) If the prime number $p > 0$ is not a Gaussian prime, then it is the product of at least two Gaussian primes (by UFT):

$$p = \pi_1 \dots \pi_r, \qquad \text{where} \qquad r \ge 2. \tag{2a}$$

Taking the norms, we obtain

$$p^2 = N(p) = N(\pi_1) \dots N(\pi_r). \tag{2b}$$

Every $N(\pi_i) > 1$ since π_i is neither 0, nor a unit. The integer p^2 has only one decomposition into the product of two integers greater than 1: $p^2 = p \cdot p$. Therefore, there are only two factors on the RHS of (2a), so the same is true for (2b), too:

$$p = \pi_1 \pi_2, \qquad \text{where} \qquad N(\pi_1) = N(\pi_2) = p.$$

Finally,

$$p = \pi_1 \pi_2 \qquad \text{and} \qquad p = N(\pi_1) = \pi_1 \overline{\pi_1}$$

imply $\pi_2 = \overline{\pi_1}$. ■

And now, here is the "list" of Gaussian primes (ε denotes any unit):

(A) $\varepsilon(1+i)$;

(B) εq where q is a positive prime number of the form $4k-1$;

(C) π where $N(\pi)$ is a positive prime number of the form $4k+1$; to each such prime number, there belong two Gaussian primes (apart from unit factors) which are complex conjugates but not associates.

Examples:

$-1+i=i(1+i)$ and $-7i$ are Gaussian primes.

Also $2-5i$ is a Gaussian prime since $(2-5i)(2+5i)=29$ and 29 is a positive prime number of the form $4k+1$.

Also $2+5i$ is a Gaussian prime which is not an associate of $2-5i$.

The factors of the decomposition $29=(5-2i)(5+2i)$ can only be associates of the previous two Gaussian primes (by the Fundamental Theorem of Arithmetic); $5-2i=(-i)(2+5i)$ and $5+2i=i(2-5i)$, indeed.

-37 is not a Gaussian prime, as 37 is (a prime number, but) not of the form $4k-1$.

Also $9+2i$ is not a Gaussian prime because $(9+2i)(9-2i)=85$ is not a prime number.

Proof: We saw that we obtain all Gaussian primes from the factorization of positive prime numbers into the product of Gaussian primes. We get different decompositions when the positive prime number is (A) 2; has the form (B) $4k-1$; or (C) $4k+1$.

(A) Since $2=(1+i)(1-i)=(-i)(1+i)^2$, the only Gaussian prime divisor of 2 is $1+i$, apart from associates.

(B) Let q be a positive prime number of the form $4k-1$. For a proof by contradiction, we assume that q is not a Gaussian prime. Then, by statement (ii) above, there exists a Gaussian prime $\pi=a+bi$ satisfying $q=N(\pi)=a^2+b^2$. This is impossible, however, as a square is congruent to 0 or 1 (mod 4), so the sum of two squares cannot be congruent to -1 (mod 4).

(C) Let p be a positive prime number of the form $4k+1$. We show first that (†) $p \mid u^2+1$ for some integer u. Consider the set $\{c,-c,c^{-1},-c^{-1}\}\subseteq \mathbf{Z}_p$ for $c\neq 0$. It can be easily checked that two such sets are either disjoint or coincide, so we get a partition of the $p-1=4k$ elements of $\mathbf{Z}_p$ into disjoint classes. Such a class contains 4 elements in general, except if two of its elements coincide. As p is odd, $v=-v$ implies $v=0$, so this cannot happen. The case $c=c^{-1}$ occurs together with $-c=-c^{-1}$ when $c^2=1$, i.e. $0=c^2-1=(c-1)(c+1)$ and this gives $c=\pm 1$ since there are no zero divisors in a field. So the class $\{1,-1\}$ consists of 2 elements. Finally $c=-c^{-1}$ occurring together with $-c=c^{-1}$ means $c^2=-1$, i.e. the integer c satisfies $p \mid c^2+1$. If this last case did not occur, then we would have one class of 2 elements whereas all other classes would be of size 4, giving altogether $4m+2$ elements, a contradiction.

Now we can show that p is not a Gaussian prime: By (†), $p \mid u^2+1=(u+i)(u-i)$ but $(u\pm i)/p=(u/p)\pm(1/p)i$ are not Gaussian integers, thus none of the factors $u+i$ and $u-i$ are divisible by p. Therefore, by definition, p is not a Gaussian prime. This means that $p=\pi\overline{\pi}$ where π and $\overline{\pi}$ are Gaussian primes. By UFT, this is the only decomposition of p into the product of Gaussian primes, apart from associates.

Finally, we have to show $\pi\neq\varepsilon\overline{\pi}$ with some unit ε. We can verify this by a simple calculation checking all cases $\varepsilon=1$, -1, i, and $-i$ for $p=a+bi$. ■

Now we are ready to prove the **Two Squares Theorem**:

Let the standard form of the positive integer n be

$$n=2^{\alpha}p_1^{\beta_1}\dots p_r^{\beta_r}q_1^{\gamma_1}\dots q_s^{\gamma_s} \tag{3}$$

where the primes p_μ are of the form $4k+1$, the primes q_ν are of the form $4k-1$, and the exponents α, β_μ, γ_ν are non-negative integers.

Then the Diophantine equation $x^2+y^2=n$ is solvable iff every γ_ν is even, and the number of solutions is $4\prod_{\mu=1}^{r}(\beta_\mu+1)$.

We consider as distinct also the solutions differing only in signs or in the order of terms. We can easily deduce also the number of "essentially" different solutions from our result.

Example: Consider $n = 4050$. Its standard form is $2 \cdot 3^4 \cdot 5^2$. The exponent of 3 is even, thus we have a solution, and the number of solutions is $4(2+1) = 12$ obtained from the exponent of 5. The solutions are

$$4050 = (\pm 45)^2 + (\pm 45)^2 = (\pm 9)^2 + (\pm 63)^2 = (\pm 63)^2 + (\pm 9)^2 \,.$$

Proof: Equation $x^2+y^2 = n$ can be rewritten as $(x+yi)(x-yi) = n$. Thus we have to determine which integers n can be factored and in how many ways into the product of two conjugate Gaussian integers.

We determine first the "standard form" of n among the Gaussian integers. By standard form, we understand a representation

$$\varepsilon \varrho_1^{\kappa_1} \dots \varrho_t^{\kappa_t}$$

where no two Gaussian primes ϱ_j are associates and ε is a unit. E.g. a standard form of 4 is $(-1)(1+i)^4$ or $(-1)(-1+i)^4$, etc. (We need the "extra" factor of unit also among the integers if we want to extend the standard form to negative integers: e.g. -9 can be represented only in the form $(-1)3^2$ or $(-1)(-3)^2$.)

Using the list of Gaussian primes, a standard form of n among the Gaussian integers is

$$n = (-i)^\alpha (1+i)^{2\alpha} \pi_1^{\beta_1} \overline{\pi_1}^{\beta_1} \dots \pi_r^{\beta_r} \overline{\pi_r}^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s} \,, \tag{4}$$

where $\pi_\mu \overline{\pi_\mu} = p_\mu$. (No two Gaussian primes on the RHS of (4) are associates.)

As $x+yi \mid n$, the standard form of $x+yi$, according to UFT, is

$$x + yi = \varepsilon (1+i)^{\alpha'} \prod_{\mu=1}^{r} \left(\pi_\mu^{\beta'_\mu} \overline{\pi_\mu}^{\beta''_\mu} \right) \prod_{\nu=1}^{s} q_\nu^{\gamma'_\nu} \tag{5}$$

where ε is a unit and each Gaussian prime occurs with an exponent not greater than in (4).

We construct a standard form of $x-yi$ by conjugating (5) and using $1-i = (-i)(1+i)$:

$$x - yi = \left(\overline{\varepsilon} (-i)^{\alpha'} \right) (1+i)^{\alpha'} \prod_{\mu=1}^{r} \left(\pi_\mu^{\beta''_\mu} \overline{\pi_\mu}^{\beta'_\mu} \right) \prod_{\nu=1}^{s} q_\nu^{\gamma'_\nu} \,. \tag{6}$$

By UFT, $(x+yi)(x-yi) = n$ iff the exponent of each Gaussian prime in (4) is the sum of the corresponding exponents in (5) and (6), and the "extra" unit factor in (4) equals the product of the unit factors in (5) and (6).

This means the following equalities:

exponent of $1+i$:	$2\alpha = \alpha' + \alpha'$	(7a)
exponent of π_μ:	$\beta_\mu = \beta'_\mu + \beta''_\mu$	(7b)
exponent of $\overline{\pi_\mu}$:	$\beta_\mu = \beta''_\mu + \beta'_\mu$	(7c)
exponent of q_ν:	$\gamma_\nu = \gamma'_\nu + \gamma'_\nu$	(7d)
unit:	$(-i)^\alpha = \varepsilon \overline{\varepsilon} (-i)^{\alpha'}$	(7e)

Equality (7a) implies $\alpha' = \alpha$, and then (7e) is true automatically for any ε. (7b) and (7c) mean the same condition which holds iff

$$\beta'_\mu = 0, 1, \dots, \beta_\mu \quad \text{and} \quad \beta''_\mu = \beta_\mu - \beta'_\mu, \quad \mu = 1, 2, \dots, r.$$

Finally, (7d) is valid iff γ_ν is even and $\gamma'_\nu = \gamma_\nu/2$.

The above imply that $x^2+y^2 = n$ is solvable iff every γ_ν is even.

The number of solutions equals the number of possible choices of ε, α', β'_μ, β''_μ, and γ'_μ. We can select these five values independently in 4, 1, $\beta_\mu+1$, 1, and 1 ways, resp., thus the number of solutions is the product of these numbers, i.e. $4\prod_{\mu=1}^{r}(\beta_\mu+1)$. ■

freudro8@gmail.com freud.web.elte.hu/bsm/index.html