A semigroup of integers and its connection with points on a circle

Grigorii Melnichenko, gmelnicenko@gmail.com
Vilnius Pedagogical University

Any number $m \geq 0$ it is possible to present as the sum of two squares. Indeed, let M be a point on a circle of the radius $r = \sqrt{m}$, then $m = a^2 + b^2$, where a, b are the coordinates of the point M. If a and a are integers, then the number $m = a^2 + b^2$ is integer. A set of the integers, which are representable as the sum of two squares is a commutative semigroup, which we denote by S. It is follows from formula

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = \left(ac - bd\right)^2 + \left(ad + bc\right)^2 .$$

The integer of the form $a = a^2 + b^2$, we name by S-number and we say that the S-number $a = a^2 + b^2$ and $b = c^2 + d^2$ are equal if $a = b$ and $c = d$. The numbers $50 = 5^2 + 5^2$ and $50 = 1^2 + 7^2$ are equal as usual numbers, but they not equal as S-numbers.

S-numbers $1_S = 1^2 + 0^2$, $-1_S = (-1)^2 + 0^2$, $i_S = 0^2 + 1^2$, $-i_S = 0^2 + (-1)^2$ form a unique group in S. We have $(-1_S)^2 = (-1_S)$ and $(i_S)^2 = -(i_S)$. So we accept 1_S as unit and i_S as imaginary unit of S. It is natural to consider the theory of divisibility of the S-numbers. Hence, we need to understand which S-numbers are prime, and which are composite. It is interesting also to find an analogue of the Unique Prime Factorization Theorem for S.