

Representing an integer as a sum of squares

Vera Serganova, Berkeley Math Circle, November 19, 2000

In how many ways can a given integer n be written as a sum of two squares? Let us start with an easier problem.

1. How many integer solutions does the equation

$$x^2 - y^2 = n$$

have depending on an integer n ?

2. Show that the equation

$$x^2 + y^2 = n$$

does not have an integer solution if $n \equiv 3 \pmod{4}$.

Denote by $S(n)$ the number of integer solutions of the equation $x^2 + y^2 = n$. Let $z = x + iy$ be a complex number with integer real and imaginary part. Such a number is called a *Gaussian integer*. The set $\mathbb{Z}[i]$ of all Gaussian integers is a *ring*, i.e. the set is equipped with addition and multiplication satisfying distributivity and associativity law.

3. Show that $S(n)$ is the number of all Gaussian integers with absolute value n . Show that if $S(n) \neq 0$ and $S(m) \neq 0$, then $S(nm) \neq 0$.

The last problem motivates us to look at the equation

$$x^2 + y^2 = p$$

for prime p . Let \mathbb{Z}_p be the set of all remainders modulo p with naturally defined addition and multiplication. Note that \mathbb{Z}_p is a ring.

4. Show that the equation $x^2 + y^2 \equiv 0 \pmod{p}$ has a non-zero solution in \mathbb{Z}_p if and only if the equation $t^2 \equiv -1 \pmod{p}$ has a solution in \mathbb{Z}_p .

Let us recall some facts about the structure of \mathbb{Z}_p . First we can divide by any non-zero element. Second, by Fermat theorem for all non-zero a

$$a^{p-1} \equiv 1 \pmod{p}$$

An element a in \mathbb{Z}_p is called primitive if every other non-zero element of \mathbb{Z}_p is a power of a . For example, 2 is *primitive* in \mathbb{Z}_{13} .

5. Show that a primitive element exists for all p and find the number of primitive elements in \mathbb{Z}_p .

6. Show that -1 is a square in \mathbb{Z}_p if $p \equiv 1 \pmod{4}$.

7. How many solutions does the equation $x^2 + y^2 \equiv 0 \pmod{p}$ have in \mathbb{Z}_p ?

8. Show that $S(p) = 8$ if $p = 4k + 1$, $S(p) = 0$ if $p = 4k + 3$, and $S(2) = 4$.

9. Let $n = 2^{k_0} p_1^{k_1} \dots p_r^{k_r} q_1^{l_1} \dots q_s^{l_s}$, where $p_i \equiv 1 \pmod{4}$ and $q_j \equiv 3 \pmod{4}$ be the prime factorization of n . Show that $S(n) \neq 0$ if and only if all l_j are even.

To obtain a formula for $S(n)$ we look again at Gaussian integers.

10. Show that all invertible elements in $\mathbb{Z}[i]$ are $\pm 1, \pm i$. Define what is a prime Gaussian integer. Which of the following are prime: $2, 3 + i, 5, 10 + i$?

We are going to prove that every Gaussian integer can be factored into primes in unique way (up to multiplication by invertible number). Let us recall our old friend Euclidean algorithm.

A ring is called *Euclidean* if one can define a non-negative function $g(a)$ on all non-zero elements such that $g(ab) \geq g(a)$ and one can divide with remainder, i.e. for any a and $b, a \neq 0$ one can write $b = qa + r$ with $g(r) < g(a)$ or $r = 0$.

11. Show that the ring of integers and the ring of polynomials are Euclidean.

12. Show that $\mathbb{Z}[i]$ is also Euclidean.

13. Show that in Euclidean rings a greatest common divisor exists and can be found by using Euclidean algorithm.

14. Show in a Euclidean ring every non-zero element is a product of primes and prime factors are defined uniquely up to multiplication by invertible elements.

Not all rings satisfy the unique factorization property.

15. Let $\mathbb{Z}[\sqrt{-3}]$ be the set of complex numbers $x + y\sqrt{-3}$ with integer x and y . Then prime factorization is not unique.

16. Show that $S(n) = 4(k_1 + 1) \dots (k_r + 1)$, assuming that k_i are as in Problem 9 and all l_j are even.

17. Show that if an integer is a sum of squares of two rational numbers, then it is a sum of two integer squares.

Let us attack another problem using the same method. Find the number of integer solutions of

$$x^2 + xy + y^2 = n.$$

18. Let $\varepsilon = (1 + \sqrt{-3})/2$, and $\mathbb{Z}[\varepsilon]$ be the ring of complex numbers $x + y\varepsilon$ with integer x and y . Such numbers may be called triangular. Draw them on the complex plane. Show that $|z|^2 = x^2 + xy + y^2$. Find all invertible elements.

19. Show that $\mathbb{Z}[\varepsilon]$ is Euclidean.

20. Show that the equation $x^2 + xy + y^2 \equiv 0 \pmod{p}$ has a non-zero solution in \mathbb{Z}_p if $p \equiv 1 \pmod{3}$ or $p = 3$.

21. The number of integer solutions of $x^2 + xy + y^2 = p$ is 12 for $p \equiv 1 \pmod{3}$. This result is harder, but you can try to prove it now.

Theorem. Any integer can be represented as a sum of four perfect squares.

22. Consider the ring $\mathbb{Z}[i, j, k]$ of all the numbers $z = x_1 + x_2i + x_3j + x_4k$, x_1, \dots, x_4 are integer, with multiplication defined by relations

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, \quad ji = -ji, \quad ik = -ki, \quad jk = -kj.$$

These are integer quaternions. Show that in general $zy \neq yz$. Let $|z| = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Show that $|zy| = |z||y|$.

23. Show that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$ has an integer solution for every p . You will probably have to do the next problem first.

24. (Minkovsky Lemma) Let L be a lattice of full rank in \mathbb{R}^n , i.e. the set of all integer linear combinations of n linearly independent vectors in \mathbb{R}^n . Let V be the volume of a minimal parallelepiped generated by vectors from L , and B be a convex body centrally symmetric with respect to the origin. If the volume of B is greater than $2^n V$ then B contains a non-zero point of the lattice.