Elementary Number Theory - Exercise 8a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

Problem 1. For each n = $1, 2, \ldots, 15$, check if n is a sum of two or three squares.

Solution 1. If we want to check whether a given n is a sum of two squares, $n = x^2 + y^2$, it suffices to check $x, y \in \{0, \ldots, \sqrt{n}\}$. Indeed, we do not need to check negative values for x, y, since replacing x with $-x$ or y with $-y$ does not change $x^2 + y^2$, and if x or y is larger than $\sqrt{n}$, then $x^2 + y^2$ is already larger than n.

We can now make a little table:

n	$n = x^2 + y^2$	$n = x^2 + y^2 + z^2$
1	$(1, 0)$	$(1, 0, 0)$
2	$(1, 1)$	$(1, 1, 0)$
3	$\times$	$(1, 1, 1)$
4	$(2, 0)$	$(2, 0, 0)$
5	$(2, 1)$	$(2, 1, 0)$
6	$\times$	$(2, 1, 1)$
7	$\times$	$\times$
8	$(2, 2)$	$(2, 2, 0)$
9	$(3, 0)$	$(3, 0, 0)$
10	$(3, 1)$	$(3, 1, 0)$
11	$\times$	$(3, 1, 1)$
12	$\times$	$(2, 2, 2)$
13	$(3, 2)$	$(3, 2, 0)$
14	$\times$	$(3, 2, 1)$
15	$\times$	$\times$

Problem 2. Write 45 and 585 as sums of two squares.
Hint: Diophantus' two squares identity.

Solution 2. Since $45 = 5 \cdot 9$ and $5 = 2^2 + 1^2$ and 9 is a square, we find

$$45 = (2^2 + 1^2) \cdot 3^2 = 6^2 + 3^2.$$

We have $225 = 45 \cdot 13$, and since both factors are sums of squares, $45 = 6^2 + 3^2$ and $13 = 3^2 + 2^2$, we obtain from Diophantus' identity that

$$585 = 45 \cdot 13 = (6^2 + 3^2)(3^2 + 2^2) = (6 \cdot 3 + 3 \cdot 2)^2 + (6 \cdot 2 - 3 \cdot 3)^2 = 24^2 + 3^2.$$

Problem 3. Show that, if n can be written as a sum of three squares, then n cannot be of the form $4^a(8b + 7)$ with non-negative integers a, b.

Solution 3. Let us suppose that $n = x^2 + y^2 + z^2$ is a sum of three squares and of the form $4^a(8b + 7)$. We distinguish the cases that n is odd or even.

- Suppose that n is odd, that is,

$$n = 8b + 7 = x^2 + y^2 + z^2.$$

Reducing modulo 8 gives

$$x^2 + y^2 + z^2 \equiv 7 \pmod 8,$$

and we want to show that this is not possible: first note that if x is even, then $x^2 \equiv 0 \pmod 8$ or $x^2 \equiv 4 \pmod 8$, and if x is odd, then $x^2 \equiv 1 \pmod 8$. From this it is easy to see that the possible values of $x^2 + y^2 + z^2 \pmod 8$ are given by $0, 1, 2, 3, 4, 5, 6$, but 7 is impossible.

- Suppose that n is even. Since n is of the form $n = 4^a(8b + 7)$, it is divisible by 4. This implies that x, y, z are all even. Indeed, since n is even, the only other possibility would be that one of them is even and the other two are odd, say $x = 2x_0$ and $y = 1 + 2y_0$ and $z = 1 + 2z_0$, but then

$$n = x^2 + y^2 + z^2 = 4x_0^2 + 1 + 4y_0 + 4y_0^2 + 1 + 4z_0 + 4z_0^2 \equiv 2 \pmod 4$$

would not be divisible by 4. Hence we can write

$$\frac{n}{4} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2,$$

and $\frac{n}{4}$ would again be of the form $4^a(8b + 7)$. We can repeat this argument until we obtain an odd number of the form $8b+7$ which is the sum of three squares, contradicting the first item.

Problem 4. We let

$$r_4(n) = \#\{(a, b, c, d) \in \mathbb{Z}^2 \,:\, n = a^2 + b^2 + c^2 + d^2\}$$

be the number of ways to write n as sum of four squares. Show that $r_4(n)$ is divisible by 8.

Solution 4. We show that every solution $n = a^2 + b^2 + c^2 + d^2$ yields at least 8 different solutions.

- If a, b, c, d are all non-zero, then we obtain (at least) the 16 different solutions

$$(\pm a, \pm b, \pm c, \pm d).$$

By permuting a, b, c, d we may get even more solutions, but if for example $a = b$, permuting a and b does not give new solutions.

- If precisely three of a, b, c, d are non-zero, say a, b, c are non-zero and $d = 0$, we obtain the 8 different solutions

$$(\pm a, \pm b, \pm c, 0).$$

Note that we can also permute a, b, c, d, and there are 4 possible positions for d, so we in fact get at least 32 different solutions.

- If precisely two of a, b, c, d are non-zero, say a, b are non-zero and $c = d = 0$, then obtain the 8 different solutions
$$(\pm a, \pm b, 0, 0), \quad (0, 0, \pm a, \pm b).$$
Again, by permuting a, b, c, d we might get even more solutions.
- If only one of a, b, c, d is non-zero, say a is non-zero and $b = c = d = 0$, then we get the 8 solutions
$$(\pm a, 0, 0, 0), \quad (0, \pm a, 0, 0), \quad (0, 0, \pm a, 0), \quad (0, 0, 0, \pm a).$$
This case also shows that $r_4(n)$ cannot always be higher power of 2 that 8. For example, we have $r_4(1) = 8$.

Problem 5. Show that every natural number can be written as a sum of five integer *cubes*. To this end, show that $n^3 \equiv n \pmod 6$, hence $n^3 - n = 6k$, and check that
$$n = n^3 + k^3 + k^3 + (-k-1)^3 + (1-k)^3.$$
Write $n = 7$ as a sum of five cubes. However, convince yourself that 7 cannot be written as a sum of five cubes of *non-negative* integers.

Solution 5. It suffices to show $n^3 \equiv n \pmod 6$ for some system of residues modulo 6, e.g. for $n \in \{0, 1, \ldots, 5\}$. In this case, it is more convenient to use $n \in \{-2, -1, 0, 1, 2, 3\}$.

Since $n^3 = n \pmod 6$, we can write $n^3 - n = 6k$ for some $k \in \mathbb{Z}$. A direct computation then shows that
$$n = n^3 + k^3 + k^3 + (-k-1)^3 + (1-k)^3,$$
so n is a sum of three cubes.

We apply this to $n = 7$. We have $7^3 = 343$, so
$$n^3 - n = 6 \cdot 56,$$
hence $k = 56$. We find
$$7 = 7^3 + 56^3 + 56^3 + (-57)^3 + (-55)^3.$$

Problem 6. Show that, if an odd prime p can be written in the form $p = x^2 + 2y^2$, then -2 is a square modulo p.

Solution 6. If $p = x^2 + 2y^2$, then x and y must be coprime to p, since otherwise p would need to both x and y, and then the right-hand side would be divisible by p^2. Writing $-2y^2 = x^2 - p$, we obtain from the properties of the Legendre symbol that
$$\left(\frac{-2}{p}\right) = \left(\frac{-2y^2}{p}\right) = \left(\frac{x^2 - p}{p}\right) = \left(\frac{x^2}{p}\right) = 1,$$
so -2 is a square modulo p. Here it is important that x and y are coprime to p.

Problem 7. Which integers n can be written in the form $n = x^2 - y^2$?

Solution 7. We claim that every odd integer n and every even integer n with $4 \mid n$ can be written in the form $n = x^2 - y^2$.

We first check that an even integer of the form $n = x^2 - y^2$ must be divisible by 4. If n is even, then x and y must either be both even or both odd. In any case, writing $n = x^2 - y^2 = (x-y)(x+y)$ we see that $x-y$ and $x+y$ are even, so n must be divisible by 4.

Next, we show that every odd integer n and every even integer n with $4 \mid n$ can be written in this form.

- If n is odd, we choose $x = \frac{n+1}{2}$ and $y = \frac{1-n}{2}$.
- If n is even and divisible by 4, we write $n = 4k$ and choose $x = k+1$ and $y = k-1$.

Problem 8 (sage)**.**

1. Write a program to find representations of an odd prime p as $p = x^2 + 2y^2$, and use it to numerically verify that p can be written in this way if and only if -2 is a square modulo p.
2. Write a program that counts $r_4(n)$. Use it to numerically verify Jacobi's formula

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d.$$