Number theory 2 2024

Exercises 2

1. Determine all quadratic residues mod 8.

Solution. We compute easily that $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 1 \bmod 8$, $4^2 = 16 \equiv 0 \bmod 8$, $5^2 = 25 \equiv 1 \bmod 8$, $6^2 = 36 \equiv 4 \bmod 8$, and $7^2 \equiv (-1)^2 = 1 \bmod 8$. Collecting the results, we see that the quadratic residues $\bmod 8$ are 0, 1 and 4.

2. Let $p > 2$ be a prime. Prove that $p \equiv 1 \bmod 4$, if -1 is a quadratic residue $\bmod p$.

Solution. Assume $p \equiv 3 \bmod 4$. In this case, $p = 4k+3$ for some $k \in \mathbb{N}$, and $\frac{p-1}{2} = 2k+1$ is odd. Assume that $x^2 \equiv -1 \bmod p$ for some $x \in \mathbb{Z}$. Fermat's little theorem implies

$$1 \equiv x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} = -1\,,$$

but this holds if and only if $p = 2$, a contradiction.

3. Let $x, y, z \in \mathbb{Z}$.

(1) Prove that $x^2 + y^2 + z^2 \not\equiv 7 \mod 8$.

(2) Let $x, y, z \in \mathbb{Z}$ such that $4 \mid x^2 + y^2 + z^2$. Prove that $x \equiv y \equiv z \equiv 0 \mod 2$.

Solution. (1) By Exercise 1, we know that the quadratic residues $\bmod 8$ are 0, 1 and 4.

4. Let $n = 4^a(8\,b+7) \in \mathbb{N}$ for some $a, b \in \mathbb{N}$. Prove that n is not the sum of three squares. This implies that the sum of three squares is congruent to one of the following

$$\begin{aligned}
0 &= 0+0+0 \equiv 4+4+0\\
1 &= 1+0+0 \equiv 4+4+1\\
2 &= 1+1+0\\
3 &= 1+1+1\\
4 &= 4+0+0 \equiv 4+4+4 \mod 8\\
5 &= 4+1+0\\
6 &= 4+1+1
\end{aligned}$$

but not 7.

5. Represent 2024 as a sum of four squares.

Solution. Note first that $2024 = 2^3{\cdot}11{\cdot}23$. It is easy to see that $8 = 2^2+2^2$, $11 = 3^2+1^2+1^2$ and $23 = 3^2 + 2^2 + 1^2 + 1^2$. Euler's Lemma[1] gives $88 = 8 \cdot 11 = 8^2 + 4^2 + 2^2 + 2^2$, and again $2024 = 88 \cdot 23 = 42^2 + 10^2 + 12^2 + 4^2$.´

[1]Lemma 8.2

There are many other solutions, for example

$$
\begin{aligned}
2024 &= 2^2 + 16^2 + 42^2 \\
&= 2^2 + 24^2 + 38^2 \\
&= 2^2 + 18^2 + 20^2 + 36^2 \,.
\end{aligned}
$$

6. Represent 29887 as a sum of four squares.

Solution. Start with the prime decomposition $29887 = 11^2 \cdot 13 \cdot 19$. Easily, $13 = 3^2 + 2^2$, $19 = 3^2 + 3^2 + 1^2$. Euler's lemma gives $13 \cdot 19 = 15^2 + 3^2 + 3^2 + 2^2$, and multiplying with the square 11^2, we have $29887 = 11^2 13 \cdot 19 = 165^2 + 33^2 + 33^2 + 22^2$.

Again, there are many solutions, for example

$$
\begin{aligned}
29887 &= 1^2 + 5^2 + 31^2 + 170^2 \\
&= 2^2 + 25^2 + 37^2 + 167^2 \\
&= 9^2 + 9^2 + 85^2 + 150^2 \,.
\end{aligned}
$$

Let $k \in \mathbb{N}^*$ and let

$$
g(k) = \inf \left\{ \ell \in \mathbb{N}^* : \forall n \in \mathbb{N} \ \exists \ x_1, x_2, \ldots, x_\ell \in \mathbb{N}^*, \text{ such that } n = \sum_{j=1}^{\ell} x_j^k \right\}.
$$

7. Prove that $g(3) \geq 9$ and $g(4) \geq 19$.

Solution. The smallest positive cubes are $1^3 = 1$, $2^3 = 8$ ja $3^3 = 27$. We see that $23 = 2^3 + 2^3 + 7 \cdot 1^1$ requires 9 cubes.

The smallest positive fourth powers are $1^4 = 1$, $2^4 = 16$ ja $3^4 = 81$. We see that $79 = 4 \cdot 2^4 + 15 \cdot 1^4$ requires 19 fourth powers.