Topics: Mostly sums of squares.

6.1. Because of Example 2.14, people keep asking: is the Jacobi symbol useless?

Definitely not. For one, it allows for easy computation of Legendre symbols, which do carry information about quadratic residues and non-residues modulo primes.

Moreover, the Jacobi symbols themselves carry **some** information, namely about quadratic **non-residues** modulo composite numbers.

Case in point: let N be a positive odd integer and prove that if the Jacobi symbol $\left(\frac{a}{N}\right)$ is -1, then a is a quadratic non-residue modulo N.

Solution. Write $N = p_1^{e_1} \dots p_r^{e_r}$ with distinct odd prime divisors. Then by the multiplicativity of the Jacobi symbol we have

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_1} \dots \left(\frac{a}{p_r}\right)^{e_r},$$

so if the product is -1 then at least one of the factors is -1, say $\left(\frac{a}{p_j}\right)^{e_j} = -1$. This implies that $\left(\frac{a}{p_j}\right) = -1$. But this is a Legendre symbol, so a is a quadratic non-residue modulo p_j, hence also a quadratic non-residue modulo N. □

6.2. Write 79 as a sum of four squares.

(You can go about this however you want, but I suggest using making the search more efficient by using the fact we mentioned that a prime p is a sum of three squares if and only if $p \not\equiv 7 \pmod 8$; so you could start by subtracting some squares from 79 and seeing if you can hit a prime of this type. Then you are reduced to a slightly simpler search.)

Solution. Using the approach hinted at in the question, we note that $79 - 6^2 = 43$, and $43 \equiv 3 \pmod 8$ is prime so it should be expressible as a sum of three squares.

Employing the same strategy, we can subtract squares from 43 until we get to a number that we know (from Theorem 2.22) is expressible as a sum of two squares:

$$\begin{aligned} 43 - 1^2 &= 42 = 2 \cdot 3 \cdot 7, \quad \text{no good} \\ 43 - 2^2 &= 39 = 3 \cdot 13, \quad \text{no good} \\ 43 - 3^2 &= 34 = 2 \cdot 17, \quad \text{good.} \end{aligned}$$

It does not take long now to see that $34 = 3^2 + 5^2$, so overall we have

$$79 = 3^2 + 3^2 + 5^2 + 6^2.$$

□

6.3. Settle the remaining case where k is even in the proof of Proposition 2.25:

Let p be prime and suppose there exist integers x, y, z, t and an even integer k such that

$$pk = x^2 + y^2 + z^2 + t^2.$$

Prove that $p\left(\frac{k}{2}\right)$ can be written as the sum of four squares.

[**Hint**: Since k is even, what are the possible combinations of even/odd among x, y, z, t? If x and y have the same parity, can you write $(x^2 + y^2)/2$ as a sum of two squares?]

Solution. Since k is even, either all of x, y, z, t are even, or all are odd, or two are even and the other two are odd. In all cases, they can be grouped in two pairs such that in each pair they have the same parity. In other words, we can relabel them so that $x \equiv y \pmod 2$ and $z \equiv t \pmod 2$.

This means that the numbers $\frac{x \pm y}{2}, \frac{z \pm t}{2}$ are integers. We can therefore write

$$p\left(\frac{k}{2}\right) = \frac{pk}{2} = \frac{x^2+y^2+z^2+t^2}{2} = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2. \qquad \square$$

6.4. Suppose a prime number p can be written as the sum of two positive integer cubes:

$$p = x^3 + y^3, \qquad x, y \in \mathbf{Z}_{\geqslant 1}.$$

Prove that $p = 2$.

Solution. We have $p = x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ and $x + y \geqslant 2$. Since p is prime we must have that $x^2 - xy + y^2 = 1$, but

$$x^2 - xy + y^2 = (x-y)^2 + xy$$

and $xy \geqslant 1$, so $x = y = 1$ and $p = 2$. $\square$

6.5. The algebraic identity in Lemma 2.16 is easy enough to verify, but where is it coming from?

Consider the complex numbers $z_1 = x + iy$ and $z_2 = w + iv$. Express the quantity $|z_1 z_2|^2$ in two ways and therefore obtain the identity

$$(x^2 + y^2)(v^2 + w^2) = (xv + yw)^2 + (xw - yv)^2.$$

Solution. We have

$$z_1 z_2 = (x + iy)(w + iv) = (xw - yv) + i(xv + yw).$$

Therefore

$$(xw - yv)^2 + (xv + yw)^2 = |z_1 z_2|^2 = |z_1|^2 |z_2|^2 = (x^2 + y^2)(w^2 + v^2). \qquad \square$$

6.6. Highly optional. After our success in Tutorial Question 6.5, we want to replicate the approach to see where the identity in Lemma 2.24 comes from.

For this we need to go beyond complex numbers.

Fix symbols $i \neq j$ satisfying the two conditions

$$i^2 = -1 = j^2, \qquad ji = -ij.$$

In particular, note that this multiplication is not commutative. However, given $r \in \mathbf{R}$, we have $ir = ri$ and $jr = rj$.

Let $k = ij$.

(a) Prove that:

$$k^2 = -1, \qquad jk = i = -kj, \qquad ki = j = -ik.$$

A *quaternion* is an expression of the form

$$\alpha = x + iy + jz + kt, \qquad \text{where } x, y, z, t \in \mathbf{R}.$$

(b) Given quaternions $\alpha = x+iy+jz+kt$ and $\beta = r+iu+jv+kw$, write out the product $\alpha\beta$ as a quaternion.

(c) Show that if $r \in \mathbf{R}$ and α is a quaternion then $r\alpha = \alpha r$.

The *conjugate* of a quaternion $\alpha = x+iy+jz+kt$ is the quaternion

$$\overline{\alpha} = x - iy - jz - kt.$$

We will take it for granted (but feel free to verify this if you want to) that

$$\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}.$$

The *reduced norm* of a quaternion $\alpha = x+iy+jz+kt$ is defined by

$$|\alpha|^2 = \alpha\overline{\alpha}.$$

(d) Prove that if $\alpha = x+iy+jz+kt$ then

$$|\alpha|^2 = x^2+y^2+z^2+t^2.$$

In particular, $|\alpha|^2 \in \mathbf{R}$.

(e) Prove that $|\alpha\beta|^2 = |\alpha|^2|\beta|^2$ for any two quaternions α, β.

(f) Use the last couple of properties to deduce the identity from Lemma 2.24:

$$\begin{aligned}&(x^2+y^2+z^2+t^2)(r^2+u^2+v^2+w^2)\\ &= (xr+yu+zv+tw)^2+(xu-yr-zw+tv)^2+(xv+yw-zr-tu)^2+(xw-yv+zu-tr)^2.\end{aligned}$$

[**Hint**: Apply part (e) with $\alpha = x-iy-jz-kt$, $\beta = r+iu+jv+kw$.]

Solution.

(a) We have:

$$\begin{aligned}
k^2 &= (ij)^2 = (ij)(ij) = i(ji)j = -i(ij)j = -i^2j^2 = (-1)(-1)(-1) = -1,\\
jk &= j(ij) = -(ij)j = -ij^2 = i\\
kj &= (ij)j = ij^2 = -i\\
ki &= (ij)i = -(ji)i = -ji^2 = j\\
ik &= i(ij) = i^2j = -j.
\end{aligned}$$

(b) This is a pain, but ends up as

$$\alpha\beta = (xr-yu-zv-tw)+i\,(xu+yr+zw-tv)+j\,(xv-yw+zr+tu)+k\,(xw+yv-zu+tr).$$

(c) This follows since we were told that $ir = ri$ and $jr = rj$.

(d) This is a particular case of part (b) with $\beta = \overline{\alpha}$.

(e) We have

$$|\alpha\beta|^2 = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\,\overline{\beta}\,\overline{\alpha} = \alpha|\beta|^2\overline{\alpha},$$

at which point we use the fact that $|\beta|^2 \in \mathbf{R}$ so it commutes with quaternions, and we continue:

$$\cdots = |\beta|^2\alpha\overline{\alpha} = |\beta|^2|\alpha|^2.$$

(f) Follow the hint. $\square$