Quadratic residues and sums of two squares

When can a positive square-free integer be written as a sum of just a few squares? The answer for four squares is "All" and for three squares "All that are not congruent to 7 (mod 8)". In this miniature we look at the positive square-free integers that can be written as the sum of two squares. We will also dally for a few lines with quadratic residues, partly to prepare us for one of the great gems of mathematics, the quadratic reciprocity theorem, to be discussed in a later miniature. In this single page there is room only for a brief outline and some details are left unjustified. The reader is invited to treat as exercises the remarks numbered as **(1)**, **(2)** etc.

Given an odd prime p, and an integer x relatively prime to p, we consider the question of whether or not there exists an integer y such that $y^2 \equiv x \pmod{p}$. If the answer is "Yes" then x is said to be a quadratic residue, otherwise it is a non-residue. **(1)** Amongst the set $\{1, 2, \ldots, p-1\}$, exactly half are quadratic residues and half are non-residues. Furthermore, **(2)** the product of two residues or **(3)** two non-residues is a quadratic residue and **(4)** the product of a residue and a non-residue is a non-residue. Since $x^{p-1} \equiv 1 \pmod{p}$, by the (little) Fermat theorem, **(5)** $x^{(p-1)/2} \equiv \pm 1 \pmod{p}$. **(6)** This can be used to distinguish quadratic residues from non-residues ($+1$: residues, -1: non-residues). Another criterion is given by

Gauss's lemma: Let $P = \{1, 2, \ldots, \frac{p-1}{2}\}$. Multiply all members of P by x and let μ be the number of these that are *not* congruent to a member of P. Then μ is even for x a quadratic residue and odd for a non-residue.

Proof: Let $Q = \{-1, -2, \ldots, -\frac{p-1}{2}\}$, then for every $y \in P$, xy is either in P or Q. Furthermore, **(7)** $xy_1 \equiv -xy_2$ is not possible for $y_1, y_2 \in P$. Hence,

$$(x) \cdot (2x) \cdot (3x) \cdot \;\cdots\; \cdot \left(\tfrac{p-1}{2}x\right) \;\equiv\; (\pm 1) \cdot (\pm 2) \cdot (\pm 3) \cdot \;\cdots\; \cdot \left(\pm \tfrac{p-1}{2}\right),$$

where μ is the number of $-$ signs in the last product. Cancel out the factors 2, 3, …, $\frac{p-1}{2}$ from both sides and we see that $x^{(p-1)/2} \equiv (-1)^\mu \pmod{p}$.

One consequence of this lemma is that -1 is a quadratic residue for an odd prime p if and only if $\frac{p-1}{2}$ is even; that is, if and only if $p \equiv 1 \pmod{4}$.

Return now to the question of which positive square-free integers n can be written as $n = x^2 + y^2$. This is clearly impossible if n is a multiple of $p \equiv 3 \pmod{4}$, because this would mean that **(8)** $z^2 = -1 \pmod{p}$, where $x \equiv yz \pmod{p}$. Hence the only possibility is that either n or $n/2$ is the product of primes of the form $p \equiv 1 \pmod{4}$. Consider first the case of n prime. The special case $n = 2$ is dealt with by $2 = 1^2 + 1^2$. For the case where $p \equiv 1 \pmod{4}$, let m denote the smallest integer satisfying $\sqrt{p} < m$ and multiply each member of the set $S = \{1, 2, \ldots, m-1\}$ by t satisfying $t^2 \equiv -1 \pmod{p}$. Let η_1, η_2, …, η_{m-1} denote the remainders when these products are divided by p. Assume these quantities are numbered in increasing order and denote the members of S by ξ_1, ξ_2, …, ξ_{m-1}, numbered in such a way that $t\xi_i \equiv \eta_i \pmod{p}$, for $i = 1, 2, \ldots, m-1$. Also write $\xi_0 = \xi_m = \eta_0 = 0$ and $\eta_m = p$. There exists $i \in \{1, 2, \ldots, m\}$ such that $\eta_i - \eta_{i-1} < m$, since otherwise

$$p = \eta_m - \eta_0 = (\eta_m - \eta_{m-1}) + (\eta_{m-1} - \eta_{m-2}) + \cdots + (\eta_1 - \eta_0) \geq m^2 > p.$$

With this choice of i, write $x = |\xi_i - \xi_{i-1}|$, $y = \eta_i - \eta_{i-1}$ so that $y \equiv \pm tx \pmod{p}$, implying that $x^2 + y^2 \equiv x^2(1 + t^2) \equiv 0 \pmod{p}$. But $0 < x^2 + y^2 < 2(m-1)^2 < 2p$, so that $x^2 + y^2 = p$.

We next establish that a square-free integer n is the sum of two squares if and only if none of its prime divisors is $\equiv 3 \pmod{4}$, generalising the case when n is prime. The extension to the more general case is easily dealt with using the identity $(x^2 + y^2)(u^2 + v^2) = (xu \mp yv)^2 + (xv \pm yu)^2$, which shows how to write mn as the sum of two squares if each of m and n can be written this way. It actually does more, because there are two solutions to this problem, if neither m nor n equals 2, even though **(9)** there cannot be more than one solution to $p = x^2 + y^2$.

Finally, we illustrate some of these results with examples. For the prime $p = 89$, it can be checked that $34^2 \equiv -1 \pmod{p}$. The value of m is 10 and the products of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ by $t = 34$ reduced $\pmod{89}$ are $\{34, 68, 13, 47, 81, 26, 60, 5, 39\}$. Sort these into increasing order and we find the values

$$\begin{aligned}
\{\xi_0, \xi_1, \xi_2, \ldots, \xi_{10}\} &= \{\, 0,\ 8,\ 3,\ 6,\ 1,\ 9,\ 4,\ 7,\ 2,\ 5,\ 0 \,\},\\
\{\eta_0, \eta_1, \eta_2, \ldots, \eta_{10}\} &= \{\, 0,\ 5,\ 13,\ 26,\ 34,\ 39,\ 47,\ 60,\ 68,\ 81,\ 89 \,\}.
\end{aligned}$$

Choose $i = 1$, because $\eta_1 - \eta_0 < 10$, and we arrive at the solution to the two-squares problem: $89 = 5^2 + 8^2$. **(10)** A similar calculation shows that $73 = 8^2 + 3^2$ and we arrive at **(11)** the two solutions to 73×89 as the sum of two squares:

$$6497 = 16^2 + 79^2 = 64^2 + 49^2.$$

John Butcher, `butcher@math.auckland.ac.nz`