Sums of squares

Recall:
THEOREM (QR PART -1): For p an odd prime, -1 is a square in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 4$.

THEOREM: An odd prime is a sum of two squares if and only if it is congruent to 1 modulo 4.

(1) Express $37, 41$, and 53 as sums of two squares.

$37 = 1^2 + 6^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$

(2) Show that every square and that every even prime is a sum of two squares.

$n^2 = n^2 + 0^2$, $2 = 1^2 + 1^2$

(3) Show[1] the "only if" direction in the theorem above.

The squares in $\mathbb{Z}_4$ are $[0]$ and $[1]$, so a number that is a sum of two squares cannot be congruent to 3 modulo 4.

(4) Proof of "if" direction:

(a) Explain why there is some natural number r with $r^2 \equiv -1 \pmod p$.

(b) Let $k = \lfloor \sqrt{p} \rfloor$ and $S = \{0, 1, \dots, k\}$. Explain why the function

$$f : S \times S \to \mathbb{Z}_p$$
$$(u, v) \mapsto [u + rv]$$

must[2] admit two input pairs $(u_1, v_1) \neq (u_2, v_2)$ such that $f(u_1, v_1) = f(u_2, v_2)$.

(c) Show that $a = u_1 - u_2$ and $b = v_1 - v_2$ satisfy $a^2 + b^2 = p$.

(a) By QR part -1, we can write $[-1] = [r]^2$ for some $[r] \in \mathbb{Z}_p$, so $r^2 \equiv -1 \pmod p$.

(b) Note that the source of f has $(k+1)^2$ elements and the target has p elements. Since $k \geq \sqrt{p}$, $k + 1 > \sqrt{p}$, so $(k + 1)^2 > p$. Thus, f cannot be injective, which yields the statement.

(c) We have $u_1 + rv_1 \equiv u_2 + rv_2 \pmod p$, so $u_1 - u_2 \equiv -r(v_1 - v_2) \pmod p$. Then

$$a^2 + b^2 \equiv (u_1 - u_2)^2 + (v_1 - v_2)^2 \equiv (u_1 - u_2)^2 + r^2(u_1 - u_2)^2 \equiv (u_1 - u_2)^2 - (u_1 - u_2)^2 \equiv 0 \pmod p.$$

---

[1] What did we do in HW#1?

[2] Hint: $k + 1 > \sqrt{p}$.

Also, $a^2 + b^2 \neq 0$, since either $u_1 - u_2 \neq 0$ or $v_1 - v_2 \neq 0$, and $a^2 + b^2 \leq 2k^2 < 2\sqrt{p}^2 = 2p$. We must have $a^2 + b^2 = p$.

SUMS OF TWO SQUARES THEOREM: A positive integer n is a sum of two squares if and only if: for every prime p such that $p \equiv 3 \pmod 4$ and p divides n, the multiplicity of p in the prime factorization of n is even.

(5) Proof of Sums of Two Squares Theorem:
  (a) Show[3] that if $q \equiv 3 \pmod 4$ is prime and divides $n = a^2 + b^2$, then q divides a and q divides b. Conclude that q^2 divides n in this case.
  (b) Use the formula $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$ to explain why any product of numbers that are sums of two squares is itself a sum of two squares.
  (c) Complete the proof of the Theorem.

[3] If $q \not| a$, show that $[b]/[a]$ is a square root of -1.

SUMS OF FOUR SQUARES THEOREM: Every positive integer n is a sum of four squares.

(5) Proof of Sums of Four Squares Theorem:

(a) Use the formula

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = (ae+bf+cg+dh)^2+(af-be+ch-dg)^2 \\ +(ag-bh-ce+df)^2+(ah+bg-cf-de)^2$$

to conclude that a product of sums of four squares is a sum of four squares. In particular, it suffices to show that every prime is a sum of four squares.

(b) Show[4] that if p is an odd prime, then there are integers x and y such that $x^2+y^2 \equiv -1 \pmod p$ and $0 \leq x, y < p/2$. Deduce that for some $k < p$ we can write kp as a sum of three (and hence four) squares.

(c) Let p be an odd prime. Suppose that the smallest $p > 0$ such that kp is a sum of four squares is greater than one. First, if k is even and $kp = a^2+b^2+c^2+d^2$, explain why we can rearrange so that $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$. Then show that

$$\frac{k}{2}p = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2$$

and deduce that k is odd.

(d) Continuing the case where p is odd, $kp = a^2+b^2+c^2+d^2$ with k minimal and odd, suppose that $k > 1$. Take a', b', c', d' such that $a' \equiv a \pmod k$ and $-m/2 < a' < m/2$, and likewise with the others. Explain why $a'^2+b'^2+c'^2+d'^2 = kr$ for some $r < k$.

(e) Continuing the previous part, use the identity from part (a) to write $(kp)(kr)$ as a sum of four squares, and show that each of numbers whose squares appear is a multiple of k. Deduce that pr is a sum of four squares, contradicting the hypothesis that $k > 1$. This concludes the proof.

[4] Hint: Show that for the sets $S = \{0^2 1^2, \dots, (\frac{p-1}{2})^2\}$ and $T = \{-1-0^2-1-1^2, \dots, -1-(\frac{p-1}{2})^2\}$ there are $s \in S$ and $t \in T$ that are congruent modulo p.