Theorem 1. The positive integer n is a sum of two squares if and only if every prime p that appears in the prime-power factorization of n and is congruent to 3, modulo 4, appears to an even power. Also, n is a sum of two relatively prime squares if and only if it is not divisible by 4 and not divisible by any prime congruent to 3, modulo 4.

Recall that if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Now let a be any integer relatively prime to p, and let $S = \{ a, 2a, 3a, \ldots, (p-1)a \}$. There are no multiples of p in this set, for each element is ab with $1 \le b \le p-1$, so p divides neither a nor b. Nor are any two of these elements congruent modulo p, for if ra and sa, $r < s$, were congruent modulo p, then $sa - ra = (s-r)a$ would be a multiple of p, but, again, $1 \le s - r < p$. So, modulo p, the elements of S are a rearrangment of the elements of $\{ 1, 2, \ldots, p-1 \}$.

It follows that

$$(a)(2a)(3a)\cdots((p-1)a) \equiv (p-1)! \pmod{p}$$
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Since $\gcd((p-1)!, p) = 1$ we can cancel $(p-1)!$ from both sides. We get Fermat's Little Theorem:

Theorem 2. If p is prime and $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$.

Now suppose p is an odd prime and $x^2 \equiv -1 \pmod{p}$. Then $\gcd(x, p) = 1$, so $(-1)^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$. But $(-1)^{(p-1)/2}$ is -1 if $p \equiv 3 \pmod{4}$. We have established the following.

Lemma 1. If p is an odd prime and $x^2 \equiv -1 \pmod{p}$ then $p \equiv 1 \pmod{4}$.

We can prove a converse to Lemma 1. First, we need Wilson's Theorem:

Theorem 3. If p is a prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Since the set S is a rearrangment, modulo p, of the elements of $\{ 1, 2, \ldots, p-1 \}$, it follows that there is an integer b, $1 \le b \le p-1$, such that $ab \equiv 1 \pmod{p}$. The congruence $a \equiv b \pmod{p}$ is then equivalent to $b^2 \equiv 1 \pmod{p}$, which is $p \mid (b+1)(b-1)$, which says $b = 1$ or $b = p-1$. Thus we can pair off each element of $\{ 1, 2, \ldots, p-1 \}$, other than 1 and $p-1$, with its multiplicative inverse, modulo p. So,

$$(p-1)! = (1)(p-1) \prod_{ab \equiv 1 \pmod{p}} ab \equiv -1 \pmod{p}$$

This proves Wilson's Theorem.

Now, there is another way to pair off the terms in $(p-1)!$, if p is odd.

$$(p-1)! = \prod_{a=1}^{(p-1)/2} a \prod_{a=(p+1)/2}^{p-1} a = \prod_{a=1}^{(p-1)/2} a \prod_{a=1}^{(p-1)/2} (p-a) = \prod_{a=1}^{(p-1)/2} a(p-a)$$
$$\equiv \prod_{a=1}^{(p-1)/2} (-a^2) = (-1)^{(p-1)/2} \left(\prod_{a=1}^{(p-1)/2} a \right)^2 \pmod{p}$$

Comparing this with Wilson's Theorem we get $(\prod_{a=1}^{(p-1)/2} a)^2 \equiv -(-1)^{(p-1)/2} \pmod{p}$. Thus we have a converse to Lemma 1:

Lemma 2. If p is prime and $p \equiv 1 \pmod 4$, then $x = \prod_{a=1}^{(p-1)/2} a$ is a solution to $x^2 \equiv -1 \pmod p$.

The next lemma says that if each of two numbers is a sum of two squares then so is their product.

Lemma 3. $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 = (ac+bd)^2 + (ad-bc)^2$.

This is proved by simply multiplying everything out. It can be interpreted as saying that if z and w are complex numbers then $|zw| = |z||w|$.

Lemma 4. If p is prime and $p \equiv 1 \pmod 4$ then p is a sum of two squares.

Proof. On the hypotheses, there exist positive integers x, y, and n such that $x^2+y^2 = np$, namely, let $y = 1$ and choose x to satisfy $x^2 \equiv -1 \pmod p$. Now we assume that n is the smallest positive integer for which $x^2 + y^2 = np$ has a solution, and prove $n = 1$. Note that we can take $0 < x < p$, from which $n < p$ follows.

Suppose $n > 1$. Define a and b by $x \equiv a \pmod n$, $-n/2 < a \leq n/2$, and $y \equiv b \pmod n$, $-n/2 < b \leq n/2$. Then $a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod n$, and $a^2 + b^2 \leq 2(n/2)^2$, so $a^2 + b^2 = mn$ with $m < n$. Also, we don't have $m = 0$ because that would imply $a = b = 0$, whence n divides both x and y, n^2 divides $x^2 + y^2$, and n divides p, impossible for $1 < n < p$. Then $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2 = (mn)(np) = mn^2p$. Working modulo n we have $ax + by \equiv x^2 + y^2 \equiv 0$, and $ay - bx \equiv xy - yx \equiv 0$, so $r = (ax + by)/n$ and $s = (ay - bx)/n$ are integers, and $r^2 + s^2 = mp$. This contradicts the minimality of n, so $n = 1$, and p is a sum of two squares.

Now we can prove Theorem 1.

If n satisfies the hypothesis, then n is a product of sums of two squares, because every prime $p \equiv 1 \pmod 4$ is a sum of two squares, and $2 = 1^2 + 1^2$, and every factor p^{2c} with $p \equiv 3 \pmod 4$ is $(p^c)^2 + 0^2$. By Lemma 3, n is a sum of two squares.

If there is a prime $p \equiv 3 \pmod 4$ dividing n, then $x^2 + y^2 \equiv 0 \pmod p$. If $y \not\equiv 0 \pmod p$, then there exists z such that $yz \equiv 1 \pmod p$, so $(xz)^2 \equiv -1 \pmod p$, but this is impossible by Lemma 1. Thus $p \mid y$, so $p \mid x$, so $p^2 \mid n$. Let p^c be the greatest power of p dividing x and y. Then $p^{2c} \mid n$, and $X^2 + Y^2 = N$, where $X = x/p^c$, $Y = y/p^c$, and

$N = n/p^{2c}$. Now p doesn't divide both X and Y, so it doesn't divide N, so the power of p dividing n is the even number, $2c$.

We have already seen that if n is divisible by a prime $p \equiv 3 \pmod 4$ then n is not a sum of relatively prime squares. If n is divisible by 4, then it can't be a sum of two odd squares (see the Pythagoras notes), so it can only be a sum of two even squares, hence, not of two relatively prime squares.

It only remains to prove that if n is a product of primes $p \equiv 1 \pmod 4$, or twice such a product, then n is a sum of relatively prime squares. This is certainly true if n is prime. If $p = a^2 + b^2$ and $p^k = c^2 + d^2$ with $\gcd(a, b) = \gcd(c, d) = 1$, then $ac + bd$ and $ac - bd$ can't both be multiples of p; if they were, their sum, $2ac$, would also be, whence either a or c would be, and if a is, then b is, and if c is, then d is, a contradiction either way. By Lemma 3 we get p^{k+1} as a sum of relatively prime squares, so, by induction, any power of a prime $p \equiv 1 \pmod 4$ is a sum of two relatively prime squares.

Now suppose $n = rs$, with $\gcd(r, s) = 1$, $r = a^2 + b^2$, $s = c^2 + d^2$, $\gcd(a, b) = \gcd(c, d) = 1$, so $n = (ac - bd)^2 + (ad + bc)^2$. We'll prove $\gcd(ac - bd, ad + bc) = 1$, completing the proof of Theorem 1. For suppose there is a prime p dividing both $ac - bd$ and $ad + bc$. It can't divide any of a, b, c, or d; if, say, $p \mid a$, then $p \mid bd$ and $p \mid bc$, so $p \mid b$, contradicting $\gcd(a, b) = 1$, or p divides both c and d, contradicting $\gcd(c, d) = 1$. Now from $p \mid ad + bc$ we get $p \mid (ac)d + bc^2$, $p \mid (bd)d + bc^2$, $p \mid (c^2 + d^2)b$, $p \mid c^2 + d^2$; also, $p \mid a^2 d + b(ac)$, $p \mid a^2 d + b(bd)$, $p \mid (a^2 + b^2)d$, $p \mid a^2 + b^2$. But this contradicts $\gcd(r, s) = 1$.