Sums of squares and Gaussian integers

Let p be an odd prime number. A number a such that $0 < a < p$, is said to be a *quadratic residue modulo p* (квадратичный вычет по модулю p) if a is congruent (сравнимо) to a perfect square (полный квадрат) modulo p, and a *quadratic nonresidue modulo p* (квадратичный невычет по модулю p) otherwise.

Exercise 1. Show that there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues modulo p.

Exercise 2. Show that -1 is a quadratic residue modulo p if and only if there exist a and b such that $a^2 + b^2$ is divisible by p.

Exercise 3. **a)** (Wilson's theorem.) Prove that $(p-1)! + 1$ is divisible by p.
b) Show that -1 is a quadratic residue modulo p if and only if $p = 4k + 1$.
Hint. x is a quadratic residue if and only if x^{-1} a quadratic residue (prove this!).

Exercise 4. Let $p = 4k + 3$. Show that if $a^2 + b^2$ is divisible by p, then both a and b are divisible by p.

Exercise 5. **a)** Show that representability of an integer as a sum of three squares is not multiplicative: find x and y such that each of them is representable as the sum of *three* squares, while xy is not representable in such a form.
b*) What about sums of four squares?

Exercise 6. Decompose the following Gaussian integers into primes in $\mathbb{Z}[i]$:
a) 13; **b)** 46; **c)** 1001; **d)** 2013; **e)** $47 + i$.

Exercise 7. How many solutions in $\mathbb{Z}$ does the equation $x^2 + y^2 = 5 \cdot 13 \cdot 17$ have?