```
theory Problem-2
  imports
    HOL−Number-Theory.Number-Theory
    Common.NT-Facts
begin
```

Positive integers p, a and b satisfy the equation $p^2 + a^2 = b^2$. Prove that if p is a prime greater than 3, then a is a multiple of 12 and $2(p + a + 1)$ is a perfect square.

```
theorem problem2:
  fixes p a b :: int
  assumes p² + a² = b²
    and p: prime p   p > 3
    and pos: a > 0   b > 0
  shows 12 dvd a
    and ∃k. k² = 2∗(p + a + 1)
proof −
  from assms(1) have ∗: p ∗ p = (b + a) ∗ (b − a)
    by (simp add: power2-eq-square flip: square-diff-square-factored)
  hence b + a dvd p ∗ p
    by auto
  have b + a ∈ {1, p, p∗p}
  proof −
    from ‹b + a dvd p∗p› obtain x y where b + a = x ∗ y and x dvd p and y
dvd p
      using dvd-productE by blast
    with ‹prime p› have |x| = 1 ∨ |x| = p and |y| = 1 ∨ |y| = p
      by (auto simp add: prime-int-iff)
    with pos ‹b + a = x ∗ y› show b + a ∈ {1, p, p∗p}
      by (cases x ≥ 0; cases y ≥ 0; auto; smt zero-less-mult-iff)
  qed
  moreover have b + a ≠ 1 using ‹a > 0› ‹b > 0› by auto
  moreover have b + a ≠ p
  proof
    assume b + a = p
    with ∗ and pos have b − a = p
      by auto
    from ‹b − a = p› and ‹b + a = p› have a = 0 by auto
    thus False using pos by auto
  qed
  ultimately have 1: b + a = p ∗ p by auto
  with ∗ pos have 2: b − a = 1 by auto

  from 1 and 2 have ∗∗: 2 ∗ a = p ∗ p − 1 by auto
  moreover have [p ∗ p = 1] (mod 24) using p by (intro pp-mod24)
    — This property is proved in Common.NT-Facts

  ultimately have 24 dvd 2∗a
    unfolding cong-def using mod-eq-dvd-iff by fastforce
```

thus *12 dvd a*
  by *auto*

from ∗∗ **have** $2*(p + a + 1) = (p + 1)^2$
  by (*auto simp add*: *ac-simps power2-sum*) (*simp add*: *power2-eq-square*)
thus $\exists k.\ k^2 = 2*(p + a + 1)$
  by *auto*
qed

end