

**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**  $p^2 + a^2 = b^2$

**and**  $p$ : *prime*  $p$   $p > 3$

**and**  $pos$ :  $a > 0$   $b > 0$

**shows**  $12 \text{ dvd } a$

**and**  $\exists k. k^2 = 2*(p + a + 1)$

**proof** –

**from**  $\langle p^2 + a^2 = b^2 \rangle$  **have**  $*$ :  $p * p = (b + a) * (b - a)$

**by** (*simp add: power2-eq-square flip: square-diff-square-factored*)

**hence**  $b + a \text{ dvd } p * p$

**by** *auto*

**have**  $b + a \in \{1, p, p*p\}$

**proof** –

**from**  $\langle b + a \text{ dvd } p*p \rangle$  **obtain**  $x\ y$  **where**

$b + a = x * y$  **and**  $x \text{ dvd } p$  **and**  $y \text{ dvd } p$

**using** *dvd-productE* **by** *blast*

**with**  $\langle \text{prime } p \rangle$  **have**  $|x| = 1 \vee |x| = p$  **and**  $|y| = 1 \vee |y| = p$

**by** (*auto simp add: prime-int-iff*)

**with**  $pos$  **and**  $\langle b + a = x * y \rangle$  **show**  $b + a \in \{1, p, p*p\}$

**by** (*cases x ≥ 0; cases y ≥ 0; auto; smt zero-less-mult-iff*)

**qed**

**moreover** **have**  $b + a \neq 1$  **using**  $\langle a > 0 \rangle \langle b > 0 \rangle$  **by** *auto*

**moreover** **have**  $b + a \neq p$

**proof**

**assume**  $b + a = p$

**with**  $*$  **and**  $pos$  **have**  $b - a = p$

**by** *auto*

**from**  $\langle b - a = p \rangle$  **and**  $\langle b + a = p \rangle$  **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**  $[p * p = 1] \text{ (mod } 24)$  **using**  $p$  **by** (*intro pp-mod24*)

— This property is proved in *Common.NT-Facts*

**ultimately** **have**  $24 \text{ dvd } 2*a$

**unfolding** *cong-def* **using** *mod-eq-dvd-iff* **by** *fastforce*

**thus**  $12 \text{ dvd } a$

**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**