36. Let p be a prime. Let m be an integer with $m \leq -(p+1)$. Prove that p is irreducible in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$.

Solution. Let p be a prime. Let m be an integer with $m \leq -(p+1)$, so that m is a negative integer. Suppose that p is reducible in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Then there exist $a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ and $c + d\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ with $a + b\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ and $c + d\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ such that

$$p = (a + b\sqrt{m})(c + d\sqrt{m}).$$

Taking the modulus of both sides, we obtain

$$p^2 = (a^2 - mb^2)(c^2 - md^2).$$

As $a^2 - mb^2$ and $c^2 - md^2$ are positive integers and p is a prime, we have

$$a^2 - mb^2 = 1, \ p \text{ or } p^2.$$

If $a^2 - mb^2 = 1$ then

$$(a + b\sqrt{m})(a - b\sqrt{m}) = 1$$

so that $a + b\sqrt{m} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$, a contradiction. If $a^2 - mb^2 = p^2$ then $c^2 - md^2 = 1$ so that

$$(c + d\sqrt{m})(c - d\sqrt{m}) = 1$$

showing that $c + d\sqrt{m} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$, a contradiction. If $a^2 - mb^2 = p$ then $b \neq 0$ (as p being a prime is not a perfect square) so that

$$p = a^2 - mb^2 \geq -mb^2 \geq (p+1)b^2 \geq p + 1 > p,$$

a contradiction. Hence p is irreducible in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. ∎