Cornacchia’s Algorithm (1908)

**Aim:** Given a positive integer $d > 0$ and a prime $p$, find an integer solution $(x, y)$ of the equation

$$x^2 + dy^2 = p. \quad (1)$$

**Procedure:**

**Step 1:** Use the modular square root algorithm to solve

$$x_0^2 \equiv -d \pmod{p}.$$ 

If no solution exists (i.e. if $(\frac{-d}{p}) = -1$), then (1) has no solution. If $x_0$ exits, then we may assume that $p/2 < x_0 < p$. (Replace $x_0$ by $p - x_0$, if necessary.)

**Step 2:** Apply the Euclidean Algorithm to $(p, x_0)$:

$$p = q_0 x_0 + r_1$$
$$x_0 = q_1 r_1 + r_2$$
$$\vdots$$
$$r_{k-2} = q_{r-1} r_{k-1} + r_k$$

Stop when $r_k \leq \lfloor \sqrt{p} \rfloor$.

**Step 3:** Put $x = r_k$, $c = \frac{p-x^2}{d}$ and $y = \sqrt{c}$. If $y \notin \mathbb{Z}$, then (1) has no solution; otherwise, $(x, y)$ is the desired solution.

**Remark:** This algorithm is easily modified to solve the equation

$$x^2 - Dy^2 = 4p,$$

where $D < 0$, $D \equiv 0, 1 \pmod{4}$; cf. H. Cohen, A Course in Computational Number Theory, p. 35.