Elliptic Curves - List 1

Task 1 (15 pts) Implement Pollard-ρ method for calculating discrete logarithms in finite groups. The implementation should work for the multiplicative group of a prime field $\mathbb{F}_p$ for p being 40-60 bit number.

Hint: To generate an instance of DLP choose a strong prime p. That is generate $p = 2\tilde{p} + 1$, where both $\tilde{p}, p$ are prime. Then generate random $g \in \mathbb{F}_p^*$ as long as $\tilde{g}$ such that

$$\tilde{g} = g^2 \bmod p$$

equals 1 (so finally $\tilde{g} \neq 1 \bmod p$). Then as the the base of the DLP take $\tilde{g}$. Note that the order of $\tilde{g}$ equals $\tilde{p}$.