

## Math 173A - Factoring

---

1. Factor 299 using Pollard's  $p - 1$  algorithm
2. Use the following data to factor  $N = 52907$ .

$$\begin{array}{llll} 399^2 \equiv 480 & (\text{mod } 52907) & \text{and} & 480 = 2^5 \cdot 3 \cdot 5 \\ 763^2 \equiv 192 & (\text{mod } 52907) & \text{and} & 192 = 2^6 \cdot 3 \\ 773^2 \equiv 15552 & (\text{mod } 52907) & \text{and} & 15552 = 2^6 \cdot 3^5 \\ 976^2 \equiv 250 & (\text{mod } 52907) & \text{and} & 250 = 2 \cdot 5^3 \end{array}$$