Discrete Logarithm and Primitive Root

Marcio Woitek

Problem 1

$$\mathrm{dlog}_{2,5}\, 3 = 3 \tag{1}$$

Problem 2

$$\mathrm{dlog}_{5,7}\, 4 = 2 \tag{2}$$

Problem 3

▷ 2

Problem 4

▷ 3
▷ 5

Problem 5

▷ Given a large modulus n, the discrete logarithm problem is computationally difficult.
▷ Using the primitive roots of a prime modulus p yields the maximum $p-1$ possible outcome values for the discrete logarithm, which is desired for cryptography.