Homework Set 8 (Lecture 29)

Problem 12

Example 23. If Bob selects $p=23$ for ElGamal, how many possible choices does he have for g?

Solution. Since g must be a primitive root modulo p, Bob has $\phi(\phi(p))=\phi(p-1)$ many choices for g. Here, Bob has $\phi(22)=10$ choices.