Homework 5

(1) For each of the following prime p, find a generator of $\mathbb{Z}_p^*$.

(a) $p = 17$

(b) $p = 29$

(c) $p = 31$

(2) If you pick any integer from $\mathbb{Z}_p^*$ randomly: what's the probability that it is a generator of $\mathbb{Z}_p^*$?

(a) $p = 17$

(b) $p = 29$

(c) $p = 31$

(3) Let $g \in G$ be a group element.

Prove that $\operatorname{ord}(g^i) = \dfrac{\operatorname{ord}(g)}{\gcd(i, \operatorname{ord}(g))}$

(4)

2.17. Use Shanks's babystep–giantstep method to solve the following discrete logarithm problems. (For (b) and (c), you may want to write a computer program implementing Shanks's algorithm.)

(a) $11^x = 21$ in $\mathbb{F}_{71}$.

(b) $156^x = 116$ in $\mathbb{F}_{593}$.

(c) $650^x = 2213$ in $\mathbb{F}_{3571}$.

(5)

2.27. Write out your own proof that the Pohlig–Hellman algorithm works in the particular case that $p - 1 = q_1 \cdot q_2$ is a product of two distinct primes. This provides a good opportunity for you to understand how the proof works and to get a feel for how it was discovered.

(6)

3.14. We stated that the number 561 is a Carmichael number, but we never checked that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad \text{and} \quad a^{561} \equiv a \pmod{17}$$

for every value of a. Then explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.