SPCS CRYPTOGRAPHY
HOMEWORK 3

Please try all the unmarked problems. #, ⋆ problems are both optional, with ⋆ problems being harder.

1. The order of a in $(\mathbb{Z}/m\mathbb{Z}, +)$ is the smallest positive integer n such that $na \equiv 0 \bmod m$. Compute the order of a in the following cases.
   (a) $a = 2$, $m = 5$.
   (b) $a = 2$, $m = 6$.
   (c) $a = 3$, $m = 6$.
   (d) $a = 3$, $m = 17$.
   In what case(s) above is a a generator of $(\mathbb{Z}/m\mathbb{Z}, +)$?

2. Compute the order of a in $\mathbb{F}_p^*$ under multiplication:
   (a) $a = 2$, $p = 5$.
   (b) $a = 2$, $p = 7$.
   (c) $a = 3$, $p = 7$.
   (d) $a = 2$, $p = 11$.
   In what case(s) above is a a primitive root $\bmod p$?

3. Compute the following,
   (a) $2^{60} \bmod 7$.
   (b) $3^{60} \bmod 7$.
   (c) $3^{60} \bmod 8$.
   (d) $3^{60} \bmod 9$.
   (e) $2^{96} \bmod 97$. (Hint: 97 is a prime.)

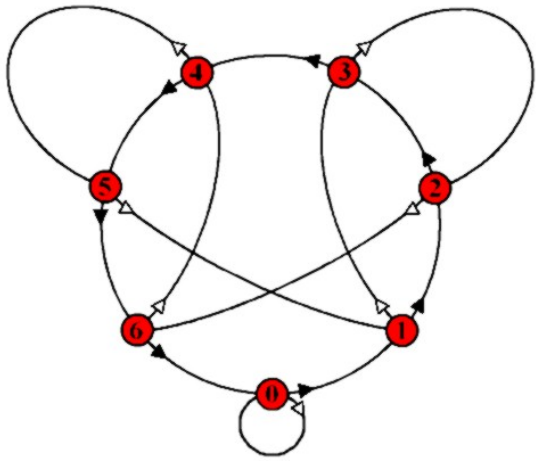
4. Let $p > 2$ be a prime, and g be a primitive root of p. Recall that $a \bmod p$ is a quadratic residue if there is some x such that $x^2 \equiv a \bmod p$, i.e. a is a square $\bmod p$.
   Prove that $a = g^k \bmod p$ in $\mathbb{F}_p^*$ is a quadratic residue modulo p if and only if k is even.

5. Let $p > 2$ be a prime, and a in $\mathbb{F}_p^*$.
   (a) Prove that $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.
   (b) If g is a primitive root $\bmod p$, show that $g^{\frac{p-1}{2}} \equiv -1 \bmod p$. (Hint: By part (a), it is either 1 or -1. Can it be 1?)
   ⋆ (c) Prove Euler's criterion:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \bmod p & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 \bmod p & \text{if } a \text{ is not a quadratic residue modulo } p \end{cases}$$

   (Hint: Use primitive roots, and Fermat's little theorem)

6. Here is a divisibility test for 7. Write down a number n. Start at the small white node at the bottom of the graph. For each digit d in n, follow d black arrows in a succession, and as you move from one digit to the next, follow 1 white arrow.



For example, if $n = 325$, follow 3 black arrows, then 1 white arrow, then 2 black arrows, then 1 white arrow, and finally 5 black arrows.

The node you end up with correspond to $n \bmod 7$. For 325, you should land at 3, meaning that $325 \equiv 3 \bmod 7$.

(a) Explain why the test works.

(b) Can you formulate a similar test for 9?

7. The following are encrypted using either Columnar cipher, Vigenere cipher, or substitution cipher. Figure out which is which. Crack them too if you like. You can assume that any Columnar cipher has a key of at most 3 characters.

(a)
```
HUKDOPSLPDHZAHSRPUNAOLPKLHVMHJABHSSFSVZPUNWLLAHO
PATLHNHPUHUKPYLHSPGLKOVDTBJOPKVUADHUAOPTAVKPLHUK
PAZUVAHIVBAAOLZWVUZVYZHUKPAZUVAHIVBADOHADPSSOHWW
LUDOLUDLNLAOVTLHUKPAZUVAQBZAAOHAPKVUADHUAAVILHSV
   ULPAZOPTPKVUVADHUAAVSVZLAOLIVFDPAOAOLIYLHK
```

(b)
```
OVPUIMFVLOFLQKQZZDZBPVWQGSXOKPHRGGRYOSCDPXSMXIMZ
XQGGKAVJPQSFWTXYPZWLTOCYWZZRHECIICOYVVMWJXYPJPYS
UCXNDCRFMPCROVPRRXMKPJDLUWQZDHPHSVXAQFFZHZKSSKRK
OGDLROSKAZUCHEFGCROVPUMZVZFNSWIAQSMXIZZROECDXOVT
QKMZZDZPFWERHVKVZWLXIOJFZFPOCMZLVFMNKEZQVMCOEVEH
        SURJIQUSYAVMCOEVEXZZPVBEHHFCBGJK
```

(c)
```
EOIWAEEURAYLHEAPARKONARTIOEEEHTPNEOOOIIREEEESRPR
OHNPMEFRVAATPNOAWAIOAENOTTEWNOERHEOWNWKGNEETTLNW
BNERDOOLIOACLEIARVWHTHRRNFNAFQNSOPTEOAPURUSPDSEL
NNNNDEHHENUFMSOEADQSFRABUTLRISTSELYHHEMNAGNNCDDL
HTRAONRUTPNAOOIFEXPHAMEAEGTNUNMEOFCAAPRNREIIHOAI
DMESRUTEFAEPNTOLTCTAWGAYCVICWNEOWTTCMSNPTRUTOEIR
GOYOSAEERDSEOCPYSACTTATDAHESLGASHHESWRNICCTALOYS
          IRUEPCPTNEHLRAMAIDTNEU
```