# Problem Set 3b

Released: September 3, 2021

1. **Extended Euclidean Algorithm.** Consider the following recursive description of Euclid's GCD algorithm.

   **function** EUCLID($a \in \mathbb{Z}^+, b \in \mathbb{Z}^+$)
       **if** $a > b$ **then return** EUCLID($b, a$) $\triangleright$ In the following, we assume $a \leq b$
       **if** $a|b$ **then**
           **return** $a$
       **else**
           $(q, r) \leftarrow$ DIVIDE($b, a$) $\triangleright$ DIVIDE($c, d$) returns $(q, r)$ such that $c = dq + r$, where $0 \leq r < |d|$
           **return** EUCLID($r, a$)

   (a) Modify the above function to return a pair of integers $(u, v)$ such that $au + bv = \gcd(a, b)$.

   (b) Compute the output of our modified function on the input pair $(1918, 2019)$.

   *Hint: You can use a table with three columns for the input $(a, b)$, the intermediate value $(q, r)$ and the output $(u, v)$, for each call to the function. You would fill the first two columns from top to bottom, and the last column in the reverse direction.*

2. Prove that $\phi(3n) = 2\phi(n)$ if and only if 3 does not divide $n$. (For this claim to hold for all $n \in \mathbb{Z}^+$, use the convention that $\phi(1) = 1$.)

3. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)$ is not divisible by 4.

4. Find all $n \in \mathbb{Z}^+$ such that $\phi(n)|n$.

5. Define the *order* of $a \in \mathbb{Z}_m^*$ to be
$$\text{ord}(a, m) = \min\{d > 0 | a^d \equiv 1 \pmod{m}\}.$$
   Prove that for every $a \in \mathbb{Z}_m^*$, $\text{ord}(a, m)|\phi(m)$.

   *Hint: Use Euler's Totient theorem. If $\text{ord}(a, m)$ does not divide $\phi(m)$, what can you say about its remainder?*

6. Define the *maximum order* in $\mathbb{Z}_m^*$ to be
$$\text{maxord}(m) = \max_{a \in \mathbb{Z}_m^*} \text{ord}(a, m).$$
   In the lectures, it was mentioned that for many $m$, $\text{maxord}(m) = \phi(m)$. In particular, this is the case when $m$ is of the form $p^k$ for odd primes $p$. In this problem you explore some cases when it is not so.

   (a) What is $\text{maxord}(8)$? Compute this by enumerating $\text{ord}(a, 8)$ for all $a \in \mathbb{Z}_8^*$.

   (b) Suppose $p, q$ are distinct primes. Let $r = \text{maxord}(p)$ and $s = \text{maxord}(q)$. Prove that $\text{maxord}(pq) = \text{lcm}(r, s)$.

   *Hint: Use CRT. To prove that $\text{maxord}(pq) = d$ you can show that $\forall a \in \mathbb{Z}_{pq}^*$, $a^d = 1$ and $\exists a \in \mathbb{Z}_{pq}^*$ s.t. $\text{ord}(a) = d$.*

   (c) Use part (b) to argue that when $p, q$ are two distinct odd primes, $\text{maxord}(p, q) \neq \phi(pq)$.

7. If possible, solve the following system of congruences using the Chinese Remainder theorem :
$$2x \equiv 11 \pmod{23}$$
$$9x \equiv 12 \pmod{31}$$
   *Hint: First write this system in a form to which CRT applies.*

8. Solve the following system of congruences :
$$2x + 5y \equiv 4 \pmod{11}$$
$$x + 3y \equiv 7 \pmod{11}$$
   *Hint: How would you solve such a system over the real or rational numbers, instead of modulo 11? You can proceed similarly, 11 being a prime.*

9. Find the last 2 digits of $2^{2018}$.

   *Hint: Note that 2 is not coprime with 100.*

10. **Square-Roots of 1.** In the lecture, we discussed the square-roots of 1 modulo a prime number.

    (a) Find all solutions of $x^2 \equiv 1 \pmod{p^k}$ where $p$ is prime and $k \geq 1$.

    *Hint: Separately analyze the cases when $p$ is odd and $p = 2$.*

    (b) Find all solutions of $x^2 \equiv 1 \pmod{144}$.