Math 453: Problem Set 4

Due at 11:00am on Wednesday, February 9, 2022

The purpose of computing is insight, not numbers. – Richard Hamming

(1) Find all complex solutions z to the following equations. You may express your answers in rectangular or polar form. Your answers should be exact and may involve trigonometric functions, complex exponentiation, and/or inverse trigonometric functions.
  (a) [3 points] $z^5 = 2 + i$.
  (b) [2 points] $z^4 + z^2 + 1 = 0$.

(2) Let $p = 123457$; note that p is prime. Compute the following exponents using the method of repeated squaring and/or other techniques. You may use a calculator or computer, but you should show your work (or your code). Do not use any built-in functions for modular exponentiation, except to check your answers. (Note that x^{y^z} means $x^{(y^z)}$, not $(x^y)^z$.)
  (a) [1 point] Calculate 2022^{2022} modulo p.
  (b) [1 point] Let $\zeta_p = e^{\frac{2\pi i}{p}}$. Compute $\zeta_p^{2022^{2022}}$.
  (c) [2 points] Assuming that $U(p)$ is cyclic, compute the order of 2022 modulo p.
  (d) [1 point] Compute $2022^{2022^{2022}}$ modulo p. (Hint: $2022^x \pmod{p}$ is a periodic function of the exponent $x \in \mathbb{Z}$. Can you think of the exponent as living in $\mathbb{Z}_n$ for some natural number n?)

(3) For $n \in \mathbb{N}$, define the **Euler phi function**

$$\varphi(n) = |\{r \in \mathbb{Z} : 0 \leq r < n \text{ and } \gcd(r, n) = 1\}|.$$

For example, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, and $\varphi(6) = 2$.
  (a) [3 points] Prove that an integer r with $0 \leq r < n$ is a generator for $\mathbb{Z}_n$ if and only if $\gcd(r, n) = 1$. Thus, $\mathbb{Z}_n$ has $\varphi(n)$ generators.
  (b) [2 points] Prove that, if $U(n)$ is cyclic, then $U(n)$ has $\varphi(\varphi(n))$ generators.

(4) Consider the following elements of S_5, written in cycle notation.

$$\sigma = (1\ 2\ 3\ 4\ 5).$$
$$\tau = (1\ 2)(3\ 4).$$

Do the following calculations by hand. If you would like to check your work, read Section 5.5 of the `html` version of the textbook and do the same calculations in Sage.
  (a) [1 point] Write σ in array form. (See Example 1.14 in the textbook for an explanation of this notation.)
  (b) [1 point] Compute $\sigma\tau$. Write your answer in cycle notation.
  (c) [1 point] Compute $\tau\sigma$. Write your answer in cycle notation.
  (d) [1 point] Compute σ^{-1} and τ^{-1}. Write your answers in cycle notation.
  (e) [1 point] Compute $\tau\sigma\tau^{-1}$. Write your answer in cycle notation.

(5) Consider a k-cycle $\sigma = (a_1\ a_2\ \cdots\ a_k) \in S_n$. Prove that, if k is even (as an integer), then σ is odd (as an element of S_n), whereas is k is odd, then σ is even. (Hint: Write σ as a product of 2-cycles.)

(6) Let $n \in \mathbb{N}$ such that $n \geq 3$. Prove that the center $Z(S_n)$ is the trivial group. (Hint: Consider a nonidentity element $\sigma \in S_n$ and two distinct numbers $a, b \in \{1, 2, \ldots, n\}$ such that $\sigma(a) = b$. Fix another number $c \in \{1, 2, \ldots, n\}$, $c \neq a$, $c \neq b$. Construct a permutation τ such that $\sigma\tau \neq \tau\sigma$.)