

Due: November 15

Solo: no collaboration allow

On this exam there are no choices (eek!). Everyone must do all five problems.

- (1) For each of the following calculations show all your work. You may use your calculator to check your answer, but I should be able to follow all your calculations without a calculator by reading your solution.
 - (a) Find $o_{193}(2)$.
 - (b) Find $14^{3664} \% 193$.
 - (c) Find $57^{-1} \pmod{193}$.
- (2) Consider the equation $10^{20000} = q(10^{100} + 3) + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 10^{100} + 3$. In this problem you will find the units digit of q .
 - (a) Show that $q \equiv 3r \pmod{10}$.
 - (b) Show that $r \equiv 10^{20000} \pmod{10^{100} + 3}$.
 - (c) Use that $10^{100} \equiv -3 \pmod{10^{100} + 3}$ to show that $r \equiv 9^{100} \pmod{10^{100} + 3}$.
 - (d) Conclude that $r = 9^{100}$. (Justify your answer.)
 - (e) Use (a) and (d) to find the units digit of q .
- (3)
 - (a) For each odd prime $p < 20$, find an integer a with $1 \leq a \leq p - 1$ and $o_p(a) = p - 1$. (It turns out that if p is prime there is always such an integer.) Be sure to show that it is indeed true that $o_p(a) = p - 1$.
 - (b) For each example you found above, compute $o_p(p - a)$. Again, be sure to justify your answers.
 - (c) Make a conjecture of the form “If p is an odd prime and $1 \leq a \leq p - 1$ and $o_p(a) = p - 1$, then $o_p(p - a) =$ fill this in.” Hint: There will be two formulas for $o_p(p - a)$, depending on whether $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.
- (4) Let a and m be integers with $m > 0$ and $\gcd(a, m) = 1$. Let $k = o_m(a)$ and consider the set
$$S = \{1, a, a^2, \dots, a^{k-1}\}.$$
 - (a) For any $n \in \mathbb{Z}$ prove that a^n is congruent modulo m to an element of S .
 - (b) Prove that no two elements of S are congruent modulo m .
 - (c) Prove that $a^{k-1} \equiv a^{-1} \pmod{m}$.
- (5)
 - (a) Let p be prime and suppose $a^2 \equiv b^2 \pmod{p}$. Prove that $a \equiv \pm b \pmod{p}$. Also, give an example to show this can be false if p is not prime.
 - (b) Suppose $\gcd(a, m) = 1$ and $a^n \equiv 1 \pmod{m}$. Prove that $o_m(a)$ divides n .