

Math 104A Test 2 SOLUTIONS 100 points February 26, 2010 Professor Evans

Directions: Except for Problem 5, show all work.

Notation: The symbol p stands for an odd prime. If a and n are relatively prime positive integers, then $\text{ord}_n(a)$ denotes the smallest positive exponent k such that $a^k \equiv 1 \pmod n$. Recall that any k for which this congruence holds is a multiple of $\text{ord}_n(a)$.

(1) How many primitive roots are there mod 81? (12 pts)

Solution: A primitive root g mod 81 has order $\phi(81) = 54$. The set of primitive roots is the set of powers g^k , where $(k, 54) = 1$. Thus there are $\phi(54) = 18$ primitive roots.

(2) Answer each part true or false, and justify in detail:

(A) 2 is a primitive root mod 59. (12 pts)

(B) -2 is a primitive root mod 59. (12 pts)

Solution: (A) 2 is not a square mod 59, since 59 is not 1 or 7 mod 8. Thus 2^{29} is not 1 mod 59. Moreover, 2^2 is also not 1 mod 59. Thus no proper divisor of 58 can be the order of 2. It follows that 2 has order 58, i.e., 2 is a primitive root mod 59. (B) Since -1 is congruent to 2^{29} by Euler's Criterion, -2 is congruent to 2^{30} mod 59. Thus -2 is a square mod 59, so it can't be a primitive root mod 59.

(3) Given that $a \equiv b \pmod p$, prove that $a^p \equiv b^p \pmod{p^2}$. (12 pts)

Solution: We have $a = b + kp$ for some k . Now raise both sides to the p -th power, and expand by the binomial theorem.

(4) Suppose that $\text{ord}_{61}(a) = 30$. Compute $\text{ord}_{61}(a^k)$ for each of the nine values $k = 1, 2, 3, 4, 5, 6, 7, 8, 9$. (9 pts)

Solution: The order of a^k is $30/(30, k)$. Thus the orders for $k = 1, 2, 3, 4, 5, 6, 7, 8, 9$ are, respectively, 30, 15, 10, 15, 6, 5, 30, 15, 10.

(5) How many solutions $x \pmod{61^4}$ are there to the congruence $x^6 - 1 \equiv 0 \pmod{61^4}$? (Answer alone suffices) (7 pts)

Solution: The congruence mod 61 has exactly 6 solutions, none of them singular. For each of the 6 solutions, there is a unique solution mod 61^4 , by the nonsingularity. Thus the answer is 6.

(6) Find three consecutive positive integers such that the first is divisible by 7, the second is divisible by 9, and the third is divisible by 11. (18 pts)

Solution: Use the CRT to solve the system $x \equiv 0 \pmod 7$, $x + 1 \equiv 0 \pmod 9$, and $x + 2 \equiv 0 \pmod{11}$. The first congruence gives $x = 7t$, and plugging this into the second, we get $7t \equiv -1 \pmod 9$. Multiply by 4 to get $t \equiv 5 \pmod 9$, so $t = 9k + 5$ and

(*) $x = 63k + 35$.

Plug this x into the third congruence to get $63k \equiv -37 \pmod{11}$. Simplify to get $8k \equiv -4 \pmod{11}$. Thus $2k \equiv -1 \pmod{11}$. Multiply by 6 to get $k \equiv 5 \pmod{11}$, i.e., $k = 11j + 5$. Plug this into (*) to get $x = 350 + 693j$. Thus 350, 351, 352 is the smallest suitable triple.

(7) Using the fact that $x \equiv 2 \pmod{11}$ is the only solution to the congruence $x^7 + 4 \equiv 0 \pmod{11}$, find all solutions to the congruence $x^7 + 4 \equiv 0 \pmod{11^2}$. (18 pts)

Let $f(x) = x^7 + 4$. A root of $f(x) = 0$ has the form $x = 2 + 11k$ for some k . By Taylor's formula, $f(2+11k) \equiv f(2) + f'(2)11k \pmod{121}$. The left side should vanish, so $11k \equiv -f(2)/f'(2) \pmod{121}$. Thus $11k \equiv -132/(7 * 2^6) \pmod{121}$. Divide by 11 to get $k \equiv -12/(7 * 2^6) \pmod{11}$. Thus $k \equiv 4 \pmod{11}$. Consequently, the root x is $2 + 11 * 4 = 46$.