

Theory of Numbers
Home Work 10, due Thursday, April 23.
Instructor: Prof. Artem Zvavitch

Problem 1. Find the order of 7 modulo 13.

Problem 2. Given that a has order kl modulo n , show that a^k has order l modulo n .

Problem 3. Let a have order $2k$ modulo the odd prime p . Show that $a^k \equiv -1 \pmod{p}$.

Problem 4. Let a have order $n - 1$ modulo n . Show that n is prime.

Problem 5. Let a have order 3 modulo prime p . Show that the order of $a + 1$ is 6.
Hint: Show first that $a^2 + a + 1 \equiv 0 \pmod{p}$ and conclude that $(a + 1)^2 \equiv a \pmod{p}$ and $(a + 1)^3 \equiv 1 \pmod{p}$.

Problem 6. Show that the odd prime divisors of $n^2 + 1$ are of the form $4k + 1$.
Hint: Let p be an odd prime divisor of $n^2 + 1$. Show that $n^2 \equiv -1 \pmod{p}$ implies that $4 \mid \varphi(p)$.

Problem 7. Show that 3 is a primitive root of 17.

Problem 8. Use previous problem to obtain all primitive roots of 17 that are less than 17.

Problem 9. Consider an odd prime p . Prove that the primitive roots of p occur in incongruent pairs r, r' where $rr' \equiv 1 \pmod{p}$.

Problem 10. Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$.