

Homework 18 – Carmichael Numbers

Recall that $n > 1$ is a Carmichael number if n is not prime but for all $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$, $a^{n-1} \equiv 1 \pmod{n}$.

- a) Prove that if n is a Carmichael number, then n is odd (hint: $a = -1$).
- b) Prove that for a composite integer n , n is a Carmichael number iff $\text{ord}_n(a) \mid n - 1$ for all $a \in \mathbf{Z}_n^*$.
- c) Suppose $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime power factorization of an odd integer n . Prove that for each i , $1 \leq i \leq k$, \mathbf{Z}_n^* has an integer of order $p_i^{e_i-1}(p_i - 1)$. (Hint: use a primitive root modulo $p_i^{e_i}$ and the Chinese Remainder Theorem.)
- d) Prove that if n is a Carmichael number, then there does not exist a prime p such that $p^2 \mid n$. (Hint: parts b and c)
- e) Prove that if $n = pq$ where p and q are odd primes, then n is not a Carmichael number. (Hint: if $p < q$, prove $p \equiv 1 \pmod{q-1}$.)

Together, this exercise proves that Carmichael numbers are odd, squarefree, and divisible by at least 3 primes. The first few examples are $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, and $2465 = 5 \cdot 17 \cdot 29$.