Algorithmic Problem Solving

Carmichael Numbers

Course code : 17ECCSE309

Tejas Arlimatti
EC Department

A little background : Fermat’s Little Theorem

- Statement : It states that if p is a prime number, then for any integer a, the number a*p – a is an integer multiple of p. In the notation of modular arithmetic, this is expressed as :

  a^p congruent to a (mod p)

Intuition : Carmichael Numbers

- In number theory, a Carmichael Number is a composite number n which satisfies the modular arithmetic congruence relation : b^{n-1} congruent to (mod n), for all integers b which are equivalently prime to n.
- Equivalently, a Carmichael Number is a composite number n for which b^n congruent to b (mod n), for all integers b.

Conclusion

- A Carmichael number will pass a Fermat primality test to every base *b* relatively prime to the number, even though it is not actually prime. This makes tests based on Fermat's Little Theorem less effective than strong probable primes tests.
- Eg : The least Carmichael number is 561, because 561 = 3 * 11 * 17, each of which is a prime number, and satisfies the Carmichael theorem easily.
- Some other examples are : 1105, 1729, 2465, 2821, 6601, etc.

Applications

- Used to understand the pattern and ordering of prime numbers.
- Cryptography requires large primes, which can be found out using this theorem.

References

- Carmichael, R. D. (1910). "Note on a new number theory function". Bulletin of the American Mathematical Society.
- Carmichael, R. D. (1912). "On composite numbers P which satisfy the Fermat congruence. American Mathematical Monthly.
- https://en.wikipedia.org/wiki/Carmichael_number