CEMC.UWATERLOO.CA | The CENTRE for EDUCATION in MATHEMATICS and COMPUTING

Grade 11/12 Math Circles March 20, 2024

Primality Testing and Integer Factorization - Problem Set

- 1. Determine whether the following statements are true.
 - $16 \equiv 51 \pmod{5}$
 - $21 \equiv 0 \pmod{7}$
 - $4 \equiv 12 \pmod{16}$
 - $-4 \equiv 12 \pmod{16}$

2. Determine whether the following equalities are true:

- $[-4] = [16] \pmod{5}$
- $[2] = [14] \pmod{7}$.
- 3. Calculate 7^{200} % 48.
- 4. Calculate 11^{301} % 1332.
- 5. Calculate 3^k % 10 , for $0 \le k \le 12$. What do you notice?
- 6. Show that if $m \ge 1$ has any odd prime factor, that $2^m + 1$ is composite.
- 7. Show that if $m \ge 1$ is composite, then $2^m 1$ is composite.
- 8. Verify that 561 is a Carmichael number.
- 9. Find the four roots of the polynomial $x^4 1 \mod 5$.
- 10. Find a modulus m such that $x^2 + 1$ has two roots.
- 11. How many bases must we choose to theoretically have a 99% chance that m is prime?