Grade 11/12 Math Circles

March 20, 2024

Primality Testing and Integer Factorization - Problem Set

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

Solution:
- $16 - 51 = -35$, which is divisible by 5, so $16 \equiv 51 \pmod 5$.
- $21 - 0 = 21$, which is divisible by 7, so $21 \equiv 0 \pmod 7$.
- $4 - 12 = -8$, which is not divisible by 16, so $4 \not\equiv 12 \pmod{16}$.
- $-4 - 12 = -16$, which is divisible by 16, so $-4 \equiv 12 \pmod{16}$.

2. Determine whether the following equalities are true:
   - $[-4] = [16] \pmod 5$
   - $[2] = [14] \pmod 7$.

Solution:
- $-4 \equiv 16 \pmod 5$, so $[-4] = [16] \pmod 5$.
- $2 \not\equiv 14 \pmod 7$, so $[2] \neq [14] \pmod 7$.

3. Calculate $7^{200} \,\%\, 48$.

Solution: Notice that $7^2 \equiv 49 \equiv 1 \pmod{48}$, so $7^{200} \equiv 49^{100} \equiv 1^{100} \equiv 1 \pmod{48}$. The remainder is 1.

4. Calculate $11^{301} \,\%\, 1332$.

Solution: Notice that $11^3 = 1331$. Thus $11^{301} \equiv 11 \times 1331^{100} \equiv 11 \times (-1)^{100} \equiv 11 \pmod{1332}$. The remainder is 11.

5. Calculate $3^k \ \% \ 10$, for $0 \leq k \leq 12$. What do you notice?

Solution: Bashing it out, we get the sequence $1, 3, 9, 7, 1, 3, 9, 7, 1, 3, 9, 7, 1$. It is periodic with period 4.

6. Show that if $m \geq 1$ has any odd prime factor, that $2^m + 1$ is composite.

Solution: Suppose $m = pk$, where p is an odd prime. Then $2^m+1 \equiv 2^{pk}+1 \equiv (2^k)^p+1 \equiv (-1)^p + 1 \equiv -1 + 1 \equiv 0 \pmod{2^k + 1}$. Therefore $2^k + 1$ divides $2^m + 1$. Since $m \geq 1$, $k \geq 1$, so $3 < 2^k + 1 < 2^m + 1$, showing that $2^k + 1$ is a proper divisor of $2^m + 1$ and that $2^m + 1$ is composite.

7. Show that if $m \geq 1$ is composite, then $2^m - 1$ is composite.

Solution: Suppose $m = jk$, where both $j, k \geq 2$. Then $2^m - 1 \equiv 2^{jk} - 1 \equiv (2^j)^k - 1 \equiv 1^k - 1 \equiv 0 \pmod{2^j - 1}$. Therefore $2^j - 1$ divides $2^m - 1$. Since $j, k \geq 2$, $3 < 2^j - 1 < 2^m - 1$, showing that $2^j - 1$ is a proper divisor of $2^m - 1$ and that $2^m - 1$ is composite.

8. Verify that 561 is a Carmichael number.

Solution: By trial factoring (remember last time!), we obtain $561 = 3 \times 11 \times 17$. Thus it is squarefree, and furthermore $3 - 1 = 2$, $11 - 1 = 10$, and $17 - 1 = 16$ all divide $561 - 1 = 560$, so 561 is Carmichael.

9. Find the four roots of the polynomial $x^4 - 1$ mod 5.

Solution: By testing out the five congruence classes, we find that $[1], [2], [3], [4]$ are all roots of $x^4 - 1$ mod 5 but that $[0]$ is not.

10. Find a modulus m such that $x^2 + 1$ has two roots.

> *Solution*: The smallest such m is 5, and the roots are [2] and [3]. You might have found this by noticing the factorization $x^4 - 1 = (x^2 - 1)(x^2 + 1)$ from the previous example.

11. How many bases must we choose to theoretically have a 99% chance that m is prime?

> *Solution*: We need to find a k such that $(1/4)^k < 1\% = 1/100$. The least such k is 4 (we have $(1/4)^3 = 1/64$ and $(1/4)^4 = 1/256$).