Grade 11/12 Math Circles

April 3, 2024

Primality Testing and Integer Factorization - Problem Set

1. Calculate 137×73 mod the following m:

$$10, 100, 1000, 10000, 100000.$$

Solution: We calculate

- $3 \times 7 \equiv 1 \pmod{10}$
- $37 \times 73 \equiv 1 \pmod{100}$
- $137 \times 73 \equiv 1 \pmod{1000}$
- $137 \times 73 \equiv 1 \pmod{10000}$
- $137 \times 73 \equiv 10001 \pmod{100000}$

2. Calculate $2^{35}, 2^{70}, 2^{140}, 2^{280}$, and $2^{560} \pmod{561}$. Hint: $2^{32} = (2^{16})^2 = ((2^8)^2)^2$ and so on. Then you can calculate 2^{35} as $2^{32} \times 8$.

Solution: We calculate

- $2^{16} \equiv (2^8)^2 \equiv 256^2 \equiv 460 \pmod{561}$
- $2^{32} \equiv (2^{16})^2 \equiv 460^2 \equiv 103 \pmod{561}$
- $2^{35} \equiv 8 \times 103 \equiv 263 \pmod{561}$
- $2^{70} \equiv 263^2 \equiv 166 \pmod{561}$
- $2^{140} \equiv 166^2 \equiv 67 \pmod{561}$
- $2^{280} \equiv 67^2 \equiv 1 \pmod{561}$
- $2^{560} \equiv 1^2 \equiv 1 \pmod{561}$

3. Are 91 and 169 coprime? Are 97 and 99 coprime?

Solution: 91 and 169 are not coprime, as they share the factor 13. 97 and 99 are coprime (in fact 97 is prime, and certainly does not divide 99).

4. Calculate inverses of 1, 2, 4, and 14 mod 15. Hint: $14 \equiv -1 \pmod{15}$.

Solution: We always have $1^{-1} \equiv 1$ mod any m. Now notice that $16 \equiv 1 \pmod{15}$. Thus $2^{-1} \equiv 8 \pmod{15}$ and $4^{-1} \equiv 4 \pmod{15}$. Finally, $14^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 14 \pmod{15}$.

5. Calculate $\phi(10)$, $\phi(15)$, and $\phi(17)$.

Solution: The set of a in $\{0, 1, 2, \ldots, 9\}$ coprime to 10 is

$$\{1, 3, 7, 9\},$$

so $\phi(10) = 4$. Similarly, we obtain the set

$$\{1, 2, 4, 7, 8, 11, 13, 14\}$$

for 15, so $\phi(15) = 8$. Since 17 is prime, every a between 1 and 16 inclusive is coprime to it, so $\phi(17) = 16$.

6. Calculate $\phi(210)$, $\phi(216)$, and $\phi(257)$. Hint: 257 is prime.

Solution: The prime factorizations are

$$\begin{aligned} 210 &= 2 \times 3 \times 5 \times 7, \\ 216 &= 2^3 \times 3^3, \\ 257 &= 257. \end{aligned}$$

We get

$$\begin{aligned}
\phi(210) &= 210 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} = 48, \\
\phi(216) &= 216 \times \frac{1}{2} \times \frac{2}{3} = 72, \\
\phi(257) &= 257 \times \frac{256}{257} = 256.
\end{aligned}$$