ELEMENTARY NUMBER THEORY - PART 2

CIPRIAN MANOLESCU

1. Some results

To a positive integer n we can associate the quantities:

$$\begin{aligned} \tau(n) &= \text{the number of positive divisors of } n, \\ \sigma(n) &= \text{the sum of positive divisors of } n, \\ \varphi(n) &= \text{the number of integers } m \text{ relatively prime to } n, \text{ with } 1 \leq m \leq n. \end{aligned}$$

The function $\varphi(n)$ is called *Euler's totient function.*

If $n = p_1^{k_1} \dots p_m^{k_m}$ is the prime factorization of n, we have the formulas:

$$\tau(n) = (k_1 + 1) \cdot \dots \cdot (k_m + 1),$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \dots \cdot \frac{p_k^{k_m+1} - 1}{p_k - 1},$$

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \dots \cdot p_m^{k_m-1}(p_m - 1).$$

Recall that we write $a \equiv b \pmod{m}$ if m divides $a - b$. By $a \pmod{m}$ we mean the remainder in the division of a by m.

Theorem 1.1 (Fermat's Little Theorem)**.** *If a is a positive integer and p is a prime, then*

$$a^p \equiv a \pmod{p}.$$

Theorem 1.2 (Euler)**.** *If a and m are relatively prime positive integers, then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Example 1.3. What is $5^{44} \pmod{49}$? We have $\varphi(49) = 7 \cdot 6 = 42$. Since 5 and 49 are relatively prime, we can apply Euler's theorem to get $5^{42} \equiv 1 \pmod{49}$. Hence:

$$5^{44} \equiv 5^2 \cdot 5^{42} \equiv 5^2 \cdot 1 \equiv 25 \pmod{49}.$$

Theorem 1.4 (Wilson)**.** *If p is a prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

2. Problems

1. Calculate: $\tau(500), \sigma(500), \varphi(500)$.

2. Calculate: $\tau(280), \sigma(280), \varphi(280)$.

3. How many even positive divisors does 1000 have? What is their sum?

4. What is the product of all positive divisors of 500?

5. If $n = p_1^{k_1} \dots p_m^{k_m}$ is the prime factorization of n, find a formula for the product of all positive divisors of n.

6. Calculate $2^{123} \pmod{11}$.

7. Calculate $2^{123} + 5^{123} \pmod{99}$.

8. Show that $\varphi(n^m) = n^{m-1} \cdot \varphi(n)$, for all $m, n \geq 1$.

9. Find the greatest common divisor of $100! + 1$ and $101!$.

10. Prove that for any even positive integer n, the number $n^2 - 1$ divides $2^{n!} - 1$.

11. Determine the last three digits of the number

$$2003^{2002^{2001}}.$$

12. Show that for any fixed positive integer n, the sequence

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \dots \pmod{n}$$

is eventually constant.