Modular Arithmetic and Arithmetic Functions

David Liu

Two toolkits for integers. **Modular shrinking:** Wilson ($(p-1)! \equiv -1 \pmod p$ for prime p) handles nearby factorials; Euler/Fermat ($a^{\varphi(m)} \equiv 1 \pmod m$ when $\gcd(a,m)=1$) cuts exponents; CRT splits a composite modulus into coprime pieces. **Arithmetic functions:** τ and φ are multiplicative — for $n = \prod p_i^{e_i}$, $\tau(n) = \prod(e_i+1)$ and $\varphi(n) = \prod p_i^{e_i-1}(p_i-1)$; inverting them means splitting the target value into admissible factors and solving for the exponents. Three examples below, then exercises.

Problem 1 (BMT 2019/5)**.** Let $2^{110} \equiv n \pmod{1111}$ with $0 \le n < 1111$. Compute n.

Solution.

$$1111 = 11 \cdot 101, \qquad 2^{10} \equiv 1 \pmod{11}, \quad 2^{100} \equiv 1 \pmod{101}$$

by Fermat, so $2^{100} \equiv 1$ modulo both, hence modulo 1111 by CRT:

$$2^{110} = 2^{100} \cdot 2^{10} \equiv 1 \cdot 1024 = 1024 \pmod{1111}.$$

□

Problem 2 (BMT 2021/6)**.** Compute the sum of all positive integers n such that n^n has 325 positive integer divisors.

Solution. With $n = \prod p_i^{e_i}$, $e_1 \le e_2 \le \cdots$, $n^n = \prod p_i^{e_i n}$:

$$325 = (e_1 n + 1)(e_2 n + 1) \cdots (e_k n + 1). \tag{$*$}$$

$325 = 5^2 \cdot 13$; the splittings into factors > 1 are

$$325, \qquad 13 \cdot 25, \qquad 5 \cdot 65, \qquad 5 \cdot 5 \cdot 13.$$

Case 325: $e_1 n = 324 = 2^2 \cdot 3^4$:

$$n = 2^x \Rightarrow x2^x = 324 \text{ (none)}; \qquad n = 3^y \Rightarrow y3^y = 324 \Rightarrow y = 4,\ n = 81.$$

Case $13 \cdot 25$: $e_1 n = 12$, $e_2 n = 24$, so $n \mid 12$ has two prime factors: $n = 6$ or 12:

$$6 = 2^1 \cdot 3^1 \text{ has exponents } (1,1) \ne (2,4) \text{ (out)}; \qquad 12 = 2^2 \cdot 3^1 \text{ (works)}.$$

Cases $5 \cdot 65$ and $5 \cdot 5 \cdot 13$: $e_1 n = 4$ with n having two or three prime factors — impossible, since $n \mid 4$.

$$12 + 81 = 93.$$

□

Problem 3 (BMT 2019/8)**.** For a positive integer n, let $\varphi(n)$ count the positive integers $\leq n$ relatively prime to n. Find the sum of all positive integers n such that $\varphi(n) = 20$.

Solution.

$$n = \prod p_i^{e_i} : \quad \varphi(n) = \prod p_i^{e_i - 1}(p_i - 1) = 20 = 2^2 \cdot 5.$$

Each $p_i - 1 \mid 20$, so $p_i \in \{2, 3, 5, 11\}$. The factor 5 of 20 must come from somewhere: among these primes only $p = 11$ has $5 \mid p - 1$, and only $p = 5$ with $e \geq 2$ has $5 \mid p^{e-1}$. Both cannot happen at once (20 has only one factor of 5), so there are two cases. We also need the small inverses $\varphi(m) = 1 \iff m \in \{1, 2\}$ and $\varphi(m) = 2 \iff m \in \{3, 4, 6\}$ (here m can only use the primes 2 and 3; check directly).

$$25 \mid n : \varphi(25) = 20 \text{ already } (125 \text{ gives } 100), \text{ so } n = 25m,\ \varphi(m) = 1 :\ n = 25,\ 50;$$
$$11 \mid n : \varphi(11) = 10\ (121 \text{ gives } 110), \text{ so } n = 11m,\ \varphi(m) = 2 :\ n = 33,\ 44,\ 66.$$

Hence

$$25 + 33 + 44 + 50 + 66 = 218.$$

□

Exercise 4. Compute the remainder when 98! is divided by 101. Hint: 1

Exercise 5 (BMT 2017/3)**.** What is the smallest positive integer with exactly 7 distinct proper divisors (divisors other than the number itself)? Hint: 2

Exercise 6 (PUMaC 2021 Number Theory #A1 / #B3)**.** Compute the remainder when $2^{3^5} + 3^{5^2} + 5^{2^3}$ is divided by 30. Hint: 3

Answers: 1024; 93; 218; 50; 24; 6.

Hints

1. Write $100! = 100 \cdot 99 \cdot 98!$ and apply Wilson's theorem to 100!.
2. Seven proper divisors means 8 divisors total. How can 8 be written as a product of integers > 1, and what does each give for the exponents?
3. Split the modulus 30 into 2, 3, and 5 and compute each term modulo each of them, then recombine. To shrink a tower like 3^5, remember that powers repeat in cycles — for example, $a^4 \equiv 1 \pmod 5$ when a shares no factor with 5.