DSBA Discrete Mathematics HW5

Kirill Korolev 203-1

21th of October, 2020

1. Find the last two digits of the number 99^{1000} in decimal notation.

   Let's use corollary from Fermat's Little Theorem that if $gcd(a, m) = 1$ and $x \equiv y\ (\varphi(m))$ then $a^x \equiv a^y\ (m)$

$$gcd(99, 1000) = 1$$
$$\varphi(100) = \varphi(5^2 \cdot 2^2) = 100(1 - \frac{1}{5})(1 - \frac{1}{2}) = 40 \Rightarrow$$
$$1000 \equiv 0\ (40) \Rightarrow 99^{1000} \equiv (99)^0 \equiv 1\ (100)$$

2. Prove that a^3 and b^3 result in the same remainder when divided by $a - b$.

   Same remainder is equivalent to $a^3 \equiv b^3\ (a - b)$ or $(a - b) \mid (a^3 - b^3)$. That's true because $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$.

3. If $11 \mid (5m + 3n)$, then $11 \mid (9m + n)$

   We need to show that if $5m \equiv -3n\,(11)$ then $9m \equiv -n\,(11)$. By the properties of congruences we need another assumption that $4m \equiv 2n\,(11)$ or because $gcd(2, 11) = 1$ we can divide by 2, then $2m \equiv n\,(11)$.

$$gcd(3, 11) = 1 \Rightarrow$$
$$5m \equiv -3n\ (11) \Rightarrow -6m \equiv -3n\ (11) \Rightarrow 2m \equiv n\ (11)$$

   That's exactly what we needed, therefore, the proof is over.

4. In a certain programming language, there is a type Int housing all integers from the range $[-M; M-1]$, where M is a large positive integer. If an integer x is out of that range (that is, there is an overflow), then x is automatically presented in Int as some other integer $I(x)$ within the range. On overflow, the value wraps around so that

$$I(x) = remainder(x + M, 2M) - M$$

   for any integer x. Prove that for every integers x and y, the following hold:

   (a) $I(x) = I(I(x))$

$$I(I(x)) = remainder(remainder(x + M, 2M) - M + M, 2M) - M =$$
$$= remainder(remainder(x + M, 2M), 2M) - M = remainder(x + M, 2M) - M = I(x)$$

   Because $remainder(remainder(x, y), y) = remainder(x, y) \quad \forall x, y \in \mathbb{Z}$ as $remainder(x, y) < y$

   (b) $I(x + y) = I(I(x) + I(y))$

$$I(I(x) + I(y)) = remainder(remainder(x + M, 2M) - M + remainder(y + M, 2M) - M + M, 2M) - M =$$
$$= remainder(remainder(x + M, 2M) + remainder(y + M, 2M) - M, 2M) - M =$$
$$= remainder(\underbrace{remainder(x + y + 2M, 2M)}_{\text{by sum of congruences}} - M, 2M) - M =$$
$$= remainder(\underbrace{remainder(x + y, 2M)}_{2M \equiv 0\ (2M)} - M, 2M) - M =$$
$$= remainder(x + y - M, 2M) - M = remainder(x + y + M, 2M) - M = I(x + y)$$

   //TODO: Add explanations

   (c) $I(xy) = I(I(x) \cdot I(y))$

$$I(I(x) \cdot I(y)) = remainder((remainder(x + M, 2M) - M)(remainder(y + M, 2M) - M) + M, 2M) - M =$$

   //TODO: Finish

5. Suppose a number $a > 1$ is divisible by 2 but not by 4. Then a has as many positive even divisors as it has positive odd divisors.

   By fundamental theorem of arithmetic we can factorize a on product of prime numbers. Condition that a is divisible by 2 but not by 4 means that 2 occurs in factorization in a first power, otherwise we'd divide by 2^2.

   $$a = 2 \cdot 3^{\alpha_1} \cdot 5^{\alpha_2} \cdot ... \cdot p^{\alpha_k}$$

   All even divisors are obtained by taking 2 and some combination of $3, 5, \dots, p$ in various powers. For example, $2, 2 \cdot 3, 2 \cdot 3^2, 2 \cdot 5, \dots$ or even the whole number as it is divisible by 2, in other words, is even. Let's count the number of combinations for even divisors.

   $$m = \alpha_1 + \alpha_2 + \ldots + \alpha_k$$
   $$C_m^0 + C_m^1 + \ldots + C_m^m = 2^m$$

   For odd divisors the sum is the same except there is no summand C_m^0, but $C_m^0 = 1$ and we don't need to forget add 1 as odd divisor, so the result is the same: $1 + C_m^1 + \ldots + C_m^m = 2^m$. Therefore, there are as many even divisors as odd ones.