Problem Set E – Partial Solutions

Shishir Agrawal

Problem 1. Come up with a rule that determines if a number is divisible by 3 using the *binary* representation of that number. State your divisibility rule clearly, using the words "if and only if." Then prove your rule.

Solution. There are probably many possible rules. Here are a couple of possibilities:

Rule 1. A number n is divisible by 3 if and only if the alternating sum of its binary digits (starting with a positive sign for its rightmost digit) is divisible by 3.

Proof. If $(a_d \cdots a_1 a_0)_2$ is the binary representation of n, then

$$n = a_d 2^d + \cdots + a_2 2^2 + a_1 2 + a_0.$$

Observe that $2 \equiv -1 \pmod 3$, so $2^k \equiv (-1)^k \pmod 3$. Thus

$$n = a_d 2^d + \cdots + a_2 2^2 + a_1 2 + a_0 \equiv (-1)^d a_d + \cdots + a_2 - a_1 + a_0 \pmod 3.$$

The right-hand side of the above congruence is the alternating sum of the binary digits of n. Thus $n \equiv 0 \pmod 3$ if and only if the alternating sum of the binary digits of n is congruent to 0 mod 3, which is what we wanted to prove.

Rule 2. A number n is divisible by 3 if and only if the difference between the number of 1s in even positions in the binary representation of n and the number of 1s in odd positions in the binary representation of n is divisible by 3.

Proof. If $(a_d \cdots a_1 a_0)_2$ is the binary representation of n, then

$$n = a_d 2^d + \cdots + a_2 2^2 + a_1 2 + a_0 = \sum_{k=0}^{d} a_k 2^k.$$

Observe that $2 \equiv -1 \pmod 3$, so

$$2^k \equiv \begin{cases} 1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases} \pmod 3.$$

Thus

$$n = \sum_{\text{even } k} a_k 2^k + \sum_{\text{odd } k} a_k 2^k \equiv \sum_{\text{even } k} a_k + \sum_{\text{odd } k} a_k(-1) = \sum_{\text{even } k} a_k - \sum_{\text{odd } k} a_k.$$

Notice that

$$\sum_{\text{even } k} a_k = \text{number of 1s in even positions}$$
$$\sum_{\text{odd } k} a_k = \text{number of 1s in odd positions}$$

so n is congruent mod 3 to the the difference between these numbers. Thus n is congruent to 0 mod 3 if and only if the difference between these numbers is congruent to 0 mod 3.

Problem 2. (a) Show that 3 is a primitive root of 19.

(b) Find all integers k between 1 and 19 whose order modulo 19 is 3. Explain.

Solution. To show that 3 is a primitive root, we need to show that the order k of 3 must be $\phi(19) = 18$. By theorem 8.1, we know that $k \mid \phi(19)$, so k must be 1, 2, 3, 6, 9, or 18. Let us check each of these powers of 3 in turn:

$$\begin{aligned}
3^1 &\equiv 3 \pmod{19} \\
3^2 &\equiv 9 \pmod{19} \\
3^3 &\equiv 27 \equiv 8 \pmod{19} \\
3^6 &= (3^3)^2 \equiv 8^2 = 64 \equiv 7 \pmod{19} \\
3^9 &= (3^3)^3 \equiv 8^3 \equiv 18 \equiv -1 \pmod{19} \\
3^{18} &= (3^9)^2 \equiv (-1)^2 \equiv 1 \pmod{19}
\end{aligned}$$

Thus $k = 18$.

For part (b), note that 3^h is a primitive root if and only if 3^h also has order $\phi(19)$. By the corollary to theorem 8.3, 3^h has the same order as 3 if and only if $\gcd(h, \phi(19)) = 1$. But the numbers that are relatively prime to $\phi(19) = 18$ are the following:

$$1, 3, 5, 7, 11, 13.$$

Thus every primitive root of 19 is congruent to 3^h for one of the h's in the list above.

Problem 3.

(a) If p is an odd prime divisor of $m^4 + 1$, show that $p \equiv 1 \bmod 8$.

(b) Prove that there are infinitely many primes that are congruent to 1 mod 8.

Solution. For part (a), let k be the order of m mod p. Note that $p \mid m^4 + 1$ means that

$$\begin{aligned} m^4 + 1 &\equiv 0 \pmod{p} \\ m^4 &\equiv -1 \pmod{p} \\ m^8 = (m^4)^2 &\equiv (-1)^2 = 1 \pmod{p}. \end{aligned}$$

By theorem 8.1, we know that $k \mid 8$. Thus $k = 1, 2, 4$ or 8. But if $k = 1, 2$ or 4, then $k \mid 4$, so $m^k \equiv 1 \pmod{p}$ would imply that $m^4 \equiv 1 \pmod{p}$, and we saw above that this is not true since $m^4 \equiv -1 \pmod{p}$ (and -1 is not congruent to 1, since p is odd). Thus it must be that $k = 8$. Now by theorem 8.1 again, we know that $8 \mid \phi(p) = p - 1$, which means that $p \equiv 1 \pmod{8}$.

For part (b), suppose for a contradiction that there are only finitely many primes $p_1, \ldots, p_r$ that are congruent to 1 mod 8. Let $n = (2p_1 \cdots p_r)^4 + 1$. Let p be a prime divisor of n. Notice that $2p_1 \cdots p_r$ is even, so n is odd. Thus p must also be odd. But then it is an odd prime divisor of an integer of the form $m^4 + 1$, so we know that $p \equiv 1 \pmod{8}$ from part (a). That means that $p = p_i$ for some i. Then

$$0 \equiv n = (2p_1 \cdots p_r)^4 + 1 \equiv 1 \pmod{p},$$

where the first congruence is because $p \mid n$ and the last congruence is because $p = p_i$ for some i. This is clearly a contradiction. Thus there must be infinitely many primes that are congruent to 1 mod 8.

Problem 4. Suppose p is a prime. A "cube root of 1 mod p" is a solution to the congruence

$$x^3 \equiv 1 \pmod{p}.$$

Notice that $x = 1$ is always a solution to this congruence; in other words, 1 is always a cube root of 1 mod p. Show that 1 is the *only* cube root of 1 mod p if and only if $p \not\equiv 1 \pmod{3}$. How many cube roots of 1 are there when $p \equiv 1 \pmod{3}$?

Solution. Suppose $p \equiv 1 \pmod{3}$. Then, by the corollary to theorem 8.5, there must be exactly 3 cube roots of 1. In particular, 1 is not the only cube root of 1.

Conversely, suppose x is a cube root of 1 mod p that's not congruent to 1. Let k be the order of x mod p. Since x is a cube root of 1, we know that $x^3 \equiv 1 \pmod{p}$, so $k \mid 3$ by theorem 8.1. Thus $k = 1$ or $k = 3$. But $k = 1$ would mean that $x^1 = x \equiv 1 \pmod{p}$, which contradicts our assumption that x is not congruent to 1. Thus $k = 3$. Then, by theorem 8.1 again, we know that $3 \mid \phi(p) = p - 1$, which means that $p \equiv 1 \pmod{3}$.