Math 319 Problem Set #3 – Solution 21 February 2002

---

1. (§2.1, problem 15) Find integers a_1, a_2, a_3, a_4, a_5 such that every integer x satisfies at least one of the congruences $x \equiv a_1 \pmod 2$, $x \equiv a_2 \pmod 3$, $x \equiv a_3 \pmod 4$, $x \equiv a_4 \pmod 6$, $x \equiv a_5 \pmod{12}$. Explain how you know your answer works, and, if applicable, how you found it.

Solution: All the given moduli are divisors of 12, so if we can choose the a_i so that each of the numbers $0, 1, \ldots, 11$ satisfies at least one of the congruences, then we will be finished.

(Why? If y is any integer then there exists an $x \in \{0, 1, 2, \cdots, 11\}$ such that $y \equiv x \pmod{12}$. If we have chosen the a_i as above, then x is congruent some a_i modulo 12, and so by transitivity, $y \equiv a_i \pmod{12}$. The mod-12 congruence implies any of the other congruences in this problem.)

If we take $a_1 = 0$, then all of the even numbers satisfy the first congruence.

If we take $a_2 = 1$, then in addition, the numbers 1 and 7 satisfy the second congruence. (Eight down, four remaining.)

If we take $a_3 = 1$, then in addition, the numbers 5 and 9 satisfy the congruence. Only the numbers 8 and 11 remain, and we have two more congruences to play with, so we predict victory in two moves.

Let $a_4 = 2$; that takes care of 8. Let $a_5 = 11$.

2. (a) Let p and q be primes. Prove that if $p \equiv 1 \pmod{q-1}$, then $a^p \equiv a \pmod q$ for every integer a.

Solution: Case 1: Suppose $q|a$. Then $a^p \equiv 0 \pmod q$ and $a \equiv 0 \pmod q$, so that $a^p \equiv a \pmod q$.

Case 2: Suppose $q \nmid a$. Suppose $p \equiv 1 \pmod{q-1}$. Then there is an integer k such that

$$p = k(q-1) + 1.$$

Thus

$$a^p = a^{k(q-1)}a \tag{1}$$
$$= a \cdot (a^k)^{(q-1)}. \tag{2}$$

Now since $q \nmid a$, we also know that $q \nmid a^k$, so by Fermat's little theorem, we have

$$(a^k)^{(q-1)} \equiv 1 \pmod{q}.$$

Thus from (1) and (2) above, we get

$$\begin{aligned} a^p &\equiv a \cdot (a^k)^{(q-1)} \pmod{q} \\ &\equiv a \cdot 1 \pmod{q} \\ &\equiv a \pmod{q} \end{aligned}$$

as required. ∎

(b) (§2.1, problem 20) Use the result in part (2a) to prove that $n^7 - n$ is divisible by 42 for any integer n.

Proof: Since $42 = [2, 3, 7]$, the result will follow if we can show that 2, 3, and 7 all divide $n^7 - n$ for every integer n. That is, we need to show $n^7 - n \equiv 0$ modulo 2, 3, and 7.

We observe that 7 is congruent to 1 modulo $(2-1)$, modulo $(3-1)$, and modulo $(7-1)$, so by the result above, the congruences

$$\begin{aligned} n^7 &\equiv n \pmod{2} \\ n^7 &\equiv n \pmod{3} \\ n^7 &\equiv n \pmod{7} \end{aligned}$$

all hold for every integer n. ∎

3. (§2.1, problem 27) Prove that $\dfrac{n^5}{5} + \dfrac{n^3}{3} + \dfrac{7n}{15}$ is an integer for every integer n.

Proof: Rewriting the given expression with a common denominator, we get

$$\frac{3n^5 + 5n^3 + 7n}{15}.$$

Our task is thus to prove that $3n^5 + 5n^3 + 7n \equiv 0 \pmod{15}$ for every integer n. This will follow if we can establish the two congruences

$$\begin{aligned} 3n^5 + 5n^3 + 7n &\equiv 0 \pmod{3} \\ 3n^5 + 5n^3 + 7n &\equiv 0 \pmod{5}. \end{aligned}$$

Using the properties of congruences, we have

$$3n^5 + 5n^3 + 7n \equiv 2n^3 + n \pmod{3}.$$

By Theorem 2.8, for any integer n, $n^3 \equiv n \pmod 3$, from which it follows that

$$2n^3 + n \equiv 2n + n \equiv 3n \equiv 0 \pmod 3,$$

and we have shown that $3n^5 + 5n^3 + 7n \equiv 0 \pmod 3$.

Similarly,

$$3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n \pmod 5,$$

and again by Theorem 2.8, $n^5 \equiv n \pmod 5$ for any n, so that

$$3n^2 + 2n \equiv 3n + 2n \equiv 5n \equiv 0 \pmod 5.$$

We have shown that for any integer n, $3n^5 + 5n^3 + 7n \equiv 0 \pmod 5$.

Since $3n^5 + 5n^3 + 7n$ is a multiple of both 3 and 5, it must also be a multiple of $[3, 5]$, and since $(3, 5) = 1$, we know that $[3, 5] = 15$. Thus $3n^5 + 5n^3 + 7n$ is divisible by 15 for any integer n, and the proof is complete. ■

4. (§2.1, problem 46) Show that for any prime p, if $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$.

Proof: Suppose $a^p \equiv b^p \pmod p$. From Theorem 2.8, we know that

$$a^p \equiv a \pmod p \text{ and } b^p \equiv b \pmod p,$$

even if p happens to divide a or b. From this it follows that $a \equiv b \pmod p$, that is $p|(a - b)$.

Now we have the factorization

$$(a - b)(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1}) \;=\; a^p - b^p.$$

Since $p|(a - b)$, to show that $p^2|(a^p - b^p)$, we need to show that

$$p|(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1}).$$

Since $a \equiv b \pmod p$, we have, for each i with $1 \leq i \leq p$,

$$a^{p-i}b^{i-1} \equiv a^{(p-i)+(i-1)} \equiv a^{p-1} \pmod p.$$

That is, every term in $(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1})$ is congruent to a^{p-1} modulo p. Since there are p terms in the sum, we have

$$(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1}) \;\equiv\; pa^{p-1} \pmod p.$$

But clearly $pa^{p-1} \equiv 0 \pmod p$, because $p \equiv 0 \pmod p$. It follows that p divides

$$(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1}),$$

and since p divides $(a - b)$ as well, the product

$$(a-b)(a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1}) \quad = \quad a^p - b^p$$

is divisible by p^2. Thus

$$a^p \equiv b^p \pmod p$$

and the proof is complete. ■

Alternate Proof: Suppose $a^p \equiv b^p \pmod p$. By Theorem 2.8, we know $a \equiv a^p \pmod p$ and $b \equiv b^p \pmod p$. It follows that $a \equiv b \pmod p$.

Write

$$\begin{aligned} a &= p\alpha + r_1 \\ b &= p\beta + r_2 \end{aligned}$$

where α, β, r_1, and r_2 are integers, and $0 \leq r_1, r_2 \leq p$. Then because $p|(a-b)$, it follows that $p|(r_1 - r_2)$, and since $|r_1 - r_2| < p$, we must have $r_1 = r_2$. Let r denote their common value.

Then

$$\begin{aligned} a^p &= (p\alpha + r)^p \\ &= (p\alpha)^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} (p\alpha)^{p-i} r^i \right) + r^p. \end{aligned}$$

Since $p \geq 2$, we know p^2 divides $(p\alpha)^p$.

Moreover, by an earlier problem, we know p divides $\binom{p}{i}$ for each i with $1 \leq i \leq p-1$, and certainly p divides $(p\alpha)^{p-i}$ for each i less than p. Thus p^2 divides each term of the sum

$$\sum_{i=1}^{p-1} \binom{p}{i} (p\alpha)^{p-i} r^i,$$

and so p^2 divides the entire sum. From this it follows that p^2 divides $a^p - r^p$, so we get

$$a^p \equiv r^p \pmod{p^2}.$$

By an analogous argument,

$$b^p \equiv r^p \pmod{p^2},$$

and so by Theorem 2.1(1) and (2), we get

$$a^p \equiv b^p \pmod{p^2},$$

as required. ■

5. (§2.1, problem 50) For every positive integer n, prove that there exists a (non-zero) multiple m of n whose base-ten representation contains only the digits 0 and 1. Prove that the same holds for the digits 0 and 2, for 0 and 3, and so on up to the digits 0 and 9, but for no other pair of digits.

Proof: If $n = 1$, then $n|1$, and if $n = 2$, then $n|10$.

Now suppose $n > 2$.

Suppose first that $2\not| n$ and $5\not| n$. Then $(10, n) = 1$, and by Theorem 2.8, we get

$$10^{\varphi(n)} \equiv 1 \pmod{n}.$$

Then $(10^{\varphi(n)})^k \equiv 1 \pmod{n}$ for every positive integer k, and since $\varphi(n) \geq 2$, all the numbers $k\varphi(n)$ are different, so that each of the numbers $10^{k\varphi(n)}$ is a distinct power of ten, and each is congruent to 1 modulo n.

Let $N = \sum_{k=1}^{n} 10^{k\varphi(n)}$. Then the base-ten representation of N contains exactly n ones and all the other digits are zero. Furthermore,

$$N \equiv \sum_{k=1}^{n} 10^{k\varphi(n)} \equiv \sum_{k=1}^{n} 1 \equiv n \pmod{n},$$

so that N is a non-zero multiple of N.

(Note: If n is a large prime, do not try this at home.)

Now suppose $n = 2^a 5^b m$, where m is relatively prime to 5 and 2. Then we find a number M made up of ones and zeros such that m divides M. Let $c = \max\{a, b\}$, and let $N = 10^c M$.

Then $n = 2^a 5^b m$ divides $2^c 5^c m = 10^c m$, which divides $10^c M = N$ (by Theorem 1.1(6)), so by Theorem 1.1(2), n divides N. Furthermore, since M is made up of ones and zeros, so is N.

The numbers $2N$, $3N$, $4N$, and so on satisfy the requirements of the second sentence above. ∎

Since every multiple of 10 has at least one zero in its base-ten representation, there is no way to satisfy the requirements of this claim with any pair of digits that does not contain a zero.