

Math 406 – Fall 2009 – Harry Tamvakis

PROBLEM SET 4 – Due October 1, 2009

Grader - Allen Gehret

Problems

4.10 What can primes (except 2, 3 or 5) be congruent to (mod 30)?

Proof. We proved on a previous homework that all primes (except 2, 3) are congruent to 1 or 5 (mod 6). Thus all primes greater than 5 are congruent to one of $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29\}$ (mod 30). Note that if n is greater than 5 and we have $n \equiv 5$ (mod 30) or $n \equiv 25$ (mod 30), then $5 \mid n$ and so n is composite. Thus all primes greater than 5 are congruent to one of $\{1, 7, 11, 13, 17, 19, 23, 29\}$ (mod 30). Since all of the numbers in $\{7, 11, 13, 17, 19, 23, 29\}$ are prime and so is $31 \equiv 1$ (mod 30), we cannot reduce this set any further. \square

4.12 Show that no square has as its last digit, 2, 3, 7 or 8.

Proof. Recall that the last digit of n is just the least residue (mod 10). By the division algorithm, we know that every number is of the form $n = 10q + r$ where $r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Thus we check the following cases:

$$(10q + 0)^2 \equiv 0^2 \equiv 0 \pmod{10}$$

$$(10q + 1)^2 \equiv 1^2 \equiv 1 \pmod{10}$$

$$(10q + 2)^2 \equiv 2^2 \equiv 4 \pmod{10}$$

$$(10q + 3)^2 \equiv 3^2 \equiv 9 \pmod{10}$$

$$(10q + 4)^2 \equiv 4^2 \equiv 6 \pmod{10}$$

$$(10q + 5)^2 \equiv 5^2 \equiv 5 \pmod{10}$$

$$(10q + 6)^2 \equiv 6^2 \equiv 6 \pmod{10}$$

$$(10q + 7)^2 \equiv 7^2 \equiv 9 \pmod{10}$$

$$(10q + 8)^2 \equiv 8^2 \equiv 4 \pmod{10}$$

$$(10q + 9)^2 \equiv 9^2 \equiv 1 \pmod{10}$$

We conclude that squares can have any of 0, 1, 4, 5, 6, 9 as their last digit, and thus never 2, 3, 7 or 8. \square

4.14 Show that the difference of two consecutive cubes is never divisible by 3.

Proof. The difference between two consecutive cubes will be of the form $(n + 1)^3 - n^3$ where n is an arbitrary integer. Note that

$$\begin{aligned}(n + 1)^3 - n^3 &= n^3 + 3n^2 + 3n + 1 - n^3 \\ &= 3(n^2 + n) + 1 \\ &\equiv 1 \pmod{3}.\end{aligned}$$

We conclude that $(n + 1)^3 - n^3$ is never divisible by 3. \square

4.18 A *palindrome* is a number that reads the same backward as forward. Examples are 22, 1331, and 935686539.

(a) Prove that every four-digit palindrome is divisible by 11.

Proof. Recall that $10 \equiv -1 \pmod{11}$. Let $abba$ be a four-digit palindrome. Note that

$$\begin{aligned}abba &\equiv a \cdot (-1)^4 + b \cdot (-1)^3 + b \cdot (-1)^2 + a \cdot (-1)^1 \pmod{11} \\ &\equiv a - b + b - a \pmod{11} \\ &\equiv 0 \pmod{11}.\end{aligned}$$

Thus $11 \mid abba$. \square

(b) What about six-digit palindromes?

Proof. The same is true for six-digit palindromes. This can be proved by either expanding the proof of (a) to accommodate six digits or by proving exercise 4.16 and then concluding that 11 divides all $2n$ -digit palindromes. \square

4.20 Show that for $k > 0$ and $m \geq 1$, $x \equiv 1 \pmod{m^k}$ implies $x^m \equiv 1 \pmod{m^{k+1}}$.

Proof. Recall that $x \equiv 1 \pmod{m^k}$ implies that $m^k \mid x - 1$ and thus $x - 1 = sm^k$ for some integer s . Also recall the identity

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1).$$

We also note that if $x \equiv 1 \pmod{m^k}$, then $x^r \equiv 1 \pmod{m^k}$, and that if $m^k \mid y - 1$, then $m \mid y - 1$. Note that

$$\begin{aligned} x^{m-1} + x^{m-2} + \cdots + x + 1 &\equiv \underbrace{1 + 1 + \cdots + 1 + 1}_{m \text{ times}} \pmod{m} \\ &\equiv m \pmod{m} \\ &\equiv 0 \pmod{m} \end{aligned}$$

Thus $m \mid x^{m-1} + x^{m-2} + \cdots + x + 1$. Combining this with $m^k \mid x - 1$, we get that $m^{k+1} \mid (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1) = x^m - 1$. We conclude that $x^m \equiv 1 \pmod{m^{k+1}}$. \square

5.2 Solve each of the following:

(a) $2x \equiv 1 \pmod{19}$.

Proof. Since $(2, 19) = 1$, we are expecting only one solution to this congruence. We can rewrite this as $19 \mid 2x - 1$, or rather, there exists a y such that $19y = 2x - 1$, which becomes $2x - 19y = 1$. Solving this Diophantine equation using methods from Section 3, we see that $x = 10$, $y = 1$ is a particular solution. Since 10 is the least residue $\pmod{19}$, we conclude that $x \equiv 10 \pmod{19}$ is the solution. \square

(b) $3x \equiv 1 \pmod{19}$.

Proof. Since $(3, 19) = 1$, we are expecting only one solution to the congruence. We can rewrite this as $19 \mid 3x - 1$, or rather, there exists a y such that $19y = 3x - 1$, which becomes $3x - 19y = 1$. We get $x = 13$, $y = 2$. Since 13 is the least residue $\pmod{19}$, we conclude that $x \equiv 13 \pmod{19}$ is the solution. \square

(c) $4x \equiv 6 \pmod{18}$.

Proof. Since $(4, 18) = 2 \mid 6$, we know that there are 2 solutions to this congruence. Rewriting the congruence, we get the equation $4x - 18y = 6$ which then simplifies to $2x - 9y = 3$. Solving this equation gives us $x = 6 + 9t$ and so our two solutions are $x \equiv 6, 15 \pmod{18}$. \square

(d) $20x \equiv 984 \pmod{1984}$.

Proof. Since $(20, 1984) = 4 \mid 984$, we conclude that there are 4 solutions to this congruence. They are $x \equiv 446, 942, 1438, 1934 \pmod{1984}$. \square

5.6 Construct linear congruences modulo 20 with no solutions, just one solution, and more than one solution. Can you find one with 20 solutions?

Proof. $2x \equiv 1 \pmod{20}$ has no solutions because $(2, 20) = 2$ does not divide 1. $3x \equiv 1 \pmod{20}$ has exactly one solution because $(3, 20) = 1$. $20x \equiv 0 \pmod{20}$ has 20 solutions because $(20, 20) = 20 \mid 0$. \square

5.20 How many multiples of b are there in the sequence

$$a, 2a, 3a, \dots, ba?$$

Proof. This is equivalent to asking for how many x , where $1 \leq x \leq b$, does $b \mid ax - 0$, which is further equivalent to asking how many solutions $(\text{mod } b)$ does $ax \equiv 0 \pmod{b}$ have. By a lemma from the book, there are (a, b) solutions (note that $(a, b) \mid 0$). \square

Add4.4

(a) What is the largest integer with ten distinct digits that is divisible by 9?

Proof. Luckily for us, $9 + 8 + \dots + 2 + 1 + 0 = 45$ which is divisible by 9. Thus, every 10 digit number which contains the digits 0 – 9 is divisible 9. There are $10! - 9!$ different permutations of these 10 digits (where we don't allow 0 to be the first digit), and the largest of these will be 9, 876, 543, 210. \square

(b) What is the largest integer with eight distinct digits that is divisible by 9?

Proof. It is clear that the number must contain the digits

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \setminus \{a, b\}$$

where a and b are two distinct digits whose sum is 9. There are $5 \cdot 8! - 4 \cdot 7!$ numbers of this form and the largest is 98,763,210 \square

Add4.6 Show that $a^5 \equiv a \pmod{10}$ for all a .

Proof. Note that $(-1)^5 \equiv -1 \pmod{10}$. This implies that if we know $n^5 \equiv n \pmod{10}$, then $(-n)^5 \equiv (-1)^5 n^5 \equiv -n \pmod{10}$. Thus it will suffice to prove this for $n = 0, 1, 2, 3, 4, 5$. Clearly $0^5 \equiv 0 \pmod{10}$ and $1^5 \equiv 1 \pmod{10}$. Also note that $2^2 \equiv 4 \pmod{10}$ and $2^4 \equiv 6 \pmod{10}$ and so $2^5 \equiv 2 \cdot 6 \equiv 2 \pmod{10}$. For 3, we have that $3^4 \equiv (-1)^2 \equiv 1 \pmod{10}$ and so $3^5 \equiv 3^4 \cdot 3 \equiv 3 \pmod{10}$. For 4 we have $4^2 \equiv 6 \pmod{10}$, $4^4 \equiv 6^2 \equiv 6 \pmod{10}$ which implies that $4^5 \equiv 4^4 \cdot 4 \equiv 6 \cdot 4 \equiv 4 \pmod{10}$. Lastly we have that $5^2 \equiv 5 \pmod{10}$ and $5^4 \equiv 5^2 \equiv 5 \pmod{10}$ which implies that $5^5 \equiv 5^4 \cdot 5 \equiv 5 \cdot 5 \equiv 5 \pmod{10}$. \square

Add4.10 If $n = 31, 415, 926, 535, 897$, then let

$$f(n) = 897 - 535 + 926 - 415 + 031 = 904.$$

Induce a definition for f and prove that if $7 \mid f(n)$, then $7 \mid n$; if $11 \mid f(n)$, then $11 \mid n$; and if $13 \mid f(n)$, then $13 \mid n$. Check 118,050,660 for divisibility by 2, 3, 5, 7, 11, and 13.

Proof. Write n in base 10^3 , i.e., $n = a_k 10^{3k} + a_{k-1} 10^{3(k-1)} + \dots + a_1 10^3 + a_0$ where $0 \leq a_i < 10^3$. Define $f(n) = \sum_{j=0}^k (-1)^j a_j$. Note that $1001 = 7 \cdot 11 \cdot 13$. Thus $10^3 \equiv -1 \pmod{p}$ where $p \in \{7, 11, 13\}$.

Let $p \in \{7, 11, 13\}$. Suppose that $p \mid f(n)$. Thus

$$\begin{aligned} f(n) &\equiv 0 \pmod{p} \\ &\equiv (-1)^k a_k + \dots - a_1 + a_0 \pmod{p} \\ &\equiv (10^3)^k a_k + \dots - a_1 10^3 + a_0 \pmod{p} \\ &\equiv n \pmod{p}. \end{aligned}$$

We conclude that $p \mid n$.

By inspection we see that 118,050,660 is divisible by 2, 3 and 5. Computing $f(n)$, we get $660 - 50 + 118 = 728 = 2^3 \cdot 7 \cdot 13$. Thus $7, 13 \mid 118,050,660$ but 11 does not divide 118,050,660 (because the converse of what we proved is also true). \square

A1) An old receipt has faded. It reads 88 chickens at a total of $\$x4.2y$, where x and y are unreadable digits. How much did each chicken cost?

Proof. Using our rule for 11, we have that $0 \equiv y - 2 + 4 - x \equiv 2 + y - x \pmod{11}$. The only (x, y) pairs of digits that satisfy this are $(0, 9), (2, 0), (3, 1), (4, 2), (5, 3), (6, 4), (9, 7)$. Since $2 \mid x42y$, we can further reduce to the pairs $(2, 0), (4, 2), (6, 4), (8, 6)$. However, out of the following: 2420, 4422, 6424, 8426, only 6424 is divisible by 8. Thus the chickens totaled $\$64.24$ and each chicken costed 73 cents. \square

A2) Solve the following linear congruences:

(a) $16x \equiv 27 \pmod{29}$,

Proof. Since $(16, 29) = 1$, there is only 1 solution. This solution is $x \equiv 18 \pmod{29}$. \square

(b) $20x \equiv 16 \pmod{64}$,

Proof. Since $(20, 64) = 4 \mid 16$, there are 4 solutions. They are $x \equiv 4, 20, 36, 52 \pmod{64}$. \square

(c) $22x \equiv 5 \pmod{12}$,

Proof. Since $(22, 12) = 2$ which does not divide 5, there are no solutions. \square

(d) $131x \equiv 21 \pmod{77}$.

Proof. Since $(131, 77) = 1$, there is 1 solution. This solution is $x \equiv 56 \pmod{77}$. \square

A3) a) Find the smallest positive integer n such that $n + 1, n + 2, n + 3$, and $n + 4$ are all composite.

Proof. By inspection, we find that $n = 23$. □

b) If k is any positive integer, prove that the number $k! + 1$ is followed by $k - 1$ consecutive composite integers. (Note: $k! = 1 \cdot 2 \cdot 3 \cdots k$.)

Proof. Note that $n \mid k!$ where $n \in \{2, \dots, k\}$. We claim that $\{k! + j \mid 2 \leq j \leq k\}$ is a set of $k - 1$ consecutive composite integers. Suppose that s is an arbitrary element from this set. Then s is of the form $k! + j$. Note that $j \mid k!$ and $j \mid j$, thus $j \mid k! + j = s$. Since $j \geq 2$, we have that s is composite. □

A4) Show that if a and b are integers and $a + b$ is even, then 24 divides $ab(a^2 - b^2)$.

Proof. We have two cases:

($a, b \equiv 0 \pmod{2}$) In this case, $8 \mid ab(a^2 - b^2) = ab(a + b)(a - b)$. If a or $b \equiv 0 \pmod{3}$, then we would be done, so assume not. If $a \equiv b \pmod{3}$ then $3 \mid a - b$. If $a \not\equiv b \pmod{3}$ then $3 \mid a + b$. Thus $3 \cdot 8 = 24 \mid ab(a^2 - b^2)$.

($a, b \equiv 1 \pmod{2}$) By checking cases, we find that $a^2 \equiv b^2 \equiv 1 \pmod{8}$ and thus $8 \mid (a^2 - b^2)$. The argument for why $3 \mid ab(a^2 - b^2)$ is identical to the first case. □

Extra Credit Problems.

EC1) a) Find a seven-digit number with all its digits different, which is divisible by each of its digits.

Proof. Since 0 does not divide non-zero integers, we cannot include 0. Since we have to include an even digit, we cannot include 5 either. The sum of the digits remaining equals 40 so we cannot include 4 either (because if we do not include 9, our sum of digits still must be divisible by 3). One possible number is 7392168. □

b) Does there exist an eight-digit number with the same property? Justify your answer.

Proof. No, we will not be able to include 0 or 5 and the sum of the digits in that case won't be divisible by 9. □

EC2) The number 1 is written on a blackboard. After each second the number on the blackboard is increased by the sum of its digits, producing a sequence of numbers 1, 2, 4, 8, 16, 23, 28, 38, 49, 62, ... Will the number 123456 ever be written on the blackboard?

Proof. No. $123456 \equiv 0 \pmod{3}$. $a_k \equiv (-1)^k \pmod{3}$. Prove this by induction on k . \square