

Math 406 – Fall 2009 – Harry Tamvakis

PROBLEM SET 5 – Due October 15, 2009

Grader - Allen Gehret

Problems

5.4 Solve the systems

(a) $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}$.

Proof. $x \equiv 5 \pmod{6}$. Use the Chinese Remainder Theorem. \square

(b) $x \equiv 2 \pmod{5}, 2x \equiv 3 \pmod{7}, 3x \equiv 4 \pmod{11}$

Proof. $x \equiv 82 \pmod{385}$. Use the Chinese Remainder Theorem. \square

(c) $x \equiv 31 \pmod{41}, x \equiv 59 \pmod{26}$

Proof. $x \equiv 605 \pmod{1066}$. Use the Chinese Remainder Theorem. \square

5.12 Find a multiple of 7 that leaves the remainder 1 when divided by 2, 3, 4, 5 or 6.

Proof. Rewrite this as the system $7x \equiv 1 \pmod{3}, 7x \equiv 1 \pmod{4}$ and $7x \equiv 1 \pmod{5}$. Using the Chinese Remainder Theorem we get $x \equiv 43 \pmod{60}$ and thus $43 \cdot 7 = 301$ is a solution. \square

5.17 If $x \equiv r \pmod{m}$ and $x \equiv s \pmod{m+1}$, show that $x \equiv r(m+1) - sm \pmod{m(m+1)}$.

Proof. Rewriting congruences, we have that $m \mid x - r$ and $m + 1 \mid x - s$. Multiplying both of these by the appropriate quantity, we have that $m(m + 1) \mid (x - r)(m + 1) = xm + x - rm - r$ and $m(m + 1) \mid m(x - s) = mx - ms$. Subtracting gives us $m(m + 1) \mid mx + x - rm - r - mx + sm = x - rm - r + ms$. This implies that $x \equiv r(m + 1) - sm \pmod{m(m + 1)}$. \square

6.2 What is the least residue of

$$5^{10} \pmod{11} \quad 5^{12} \pmod{11} \quad 1945^{12} \pmod{11}?$$

Proof. By Fermat's Theorem we have that $5^{11-1} = 5^{10} \equiv 1 \pmod{11}$ since $(11, 5) = 1$. Thus $5^{12} = 5^{10} \cdot 5^2 = 25 \equiv 3 \pmod{11}$. Note that $1945 \equiv 9 \pmod{11}$. Since $(9, 11) = 1$, we have that $1945^{12} \equiv 9^{12} \equiv 9^{10} \cdot 9^2 \equiv 81 \equiv 4 \pmod{11}$. \square

6.4 What are the last two digits of 7^{355} ?

Proof. Note that $7^4 = 2401 \equiv 1 \pmod{100}$. Thus we have that $7^{355} = (7^4)^{88} \cdot 7^3 \equiv 7^3 \equiv 343 \equiv 43 \pmod{100}$. Thus the last two digits of 7^{355} are 43. \square

6.15 Suppose that p is an odd prime.

(a) Show that

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

Proof. For all n , $1 \leq n \leq p-1$, we have that $(p, n) = 1$ and by Fermat's Theorem we get $n^{p-1} \equiv 1 \pmod{p}$. Thus $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv \sum_{k=1}^{p-1} 1 \equiv p-1 \equiv -1 \pmod{p}$. \square

(b) Show that

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

Proof. For all n , $1 \leq n \leq p-1$, we have that $(p, n) = 1$ and by Fermat's Theorem we get $n^p = n \cdot n^{p-1} \equiv n \pmod{p}$. Thus $1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + (p-1) \equiv 1 + (p-1) + 2 + (p-2) + \cdots + \frac{p-1}{2} + (p - \frac{p-1}{2}) \equiv p + p + \cdots + p \equiv 0 \pmod{p}$. \square

6.17 Show that for any two different primes p, q ,

(a) $pq \mid (a^{p+q} - a^{p+1} - a^{q+1} + a^2)$ for all a .

Proof. Since p, q are primes, we have that $a^p \equiv a \pmod{p}$ and $a^q \equiv a \pmod{q}$ for all a . Equivalently, $p \mid a^p - a$ and $q \mid a^q - a$. Multiplying these together gives us $pq \mid (a^p - a)(a^q - a) = a^{p+q} - a^{p+1} - a^{q+1} + a^2$.
□

(b) $pq \mid (a^{pq} - a^p - a^q + a)$ for all a .

Proof. Note that $a^{pq} - a^p \equiv (a^p)^q - a^p \equiv a^q - a \pmod{p}$ and so $p \mid a^{pq} - a^p - a^q + a$. Additionally, $a^{pq} - a^q \equiv (a^q)^p - a^q \equiv a^p - a \pmod{q}$ and so $q \mid a^{pq} - a^p - a^q + a$. Since $(p, q) = 1$, we get that $pq \mid a^{pq} - a^p - a^q + a$.
□

6.18 Show that if p is an odd prime, then $2p \mid (2^{2p-1} - 2)$.

Proof. Note that $(2, p) = 1$. Thus $2^{p-1} \equiv 1 \pmod{p}$ and so $(2^{p-1})^2 \equiv 2^{2p-2} \equiv 1 \pmod{p}$. This implies that $p \mid 2^{2p-2} - 1$. Also $2 \mid 2$. Therefore we conclude that $2p \mid 2^{2p-1} - 2$.
□

A1) From Fermat's theorem deduce that 13 divides $11^{12n+6} + 1$ for all non-negative integers n .

Proof. $11^{12n+6} \equiv 11^6 \cdot (11^{12})^n \equiv 12 \cdot 1^n \equiv -1 \pmod{13}$. Thus $13 \mid 11^{12n+6} + 1$.
□

A2) a) Find the remainder when $15!$ is divided by 17.

Proof. By Wilson's Theorem,

$$\begin{aligned} 16! &\equiv -1 \pmod{17} \\ 16 \cdot 15! &\equiv -1 \pmod{17} \\ -1 \cdot 15! &\equiv -1 \pmod{17} \\ (-1)^2 \cdot 15! &\equiv (-1)^2 \pmod{17} \\ 15! &\equiv 1 \pmod{17} \end{aligned}$$

and so $17 \mid 15! - 1$ which implies that the remainder is 1. \square

b) Find the remainder when $2(26!)$ is divided by 29.

Proof. By Wilson's Theorem we have that

$$\begin{aligned}28! &\equiv -1 \pmod{29} \\28 \cdot 27 \cdot 26! &\equiv -1 \pmod{29} \\-1 \cdot -1 \cdot 2 \cdot 26! &\equiv -1 \pmod{29} \\2 \cdot 26! &\equiv -1 \pmod{29}\end{aligned}$$

and thus $2(26!)$ leaves a remainder of 28. \square

A3) If p and q are distinct prime numbers, prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Proof. By Fermat's Theorem we have that $p^{q-1} \equiv 1 \pmod{q}$ and $q^{p-1} \equiv 1 \pmod{p}$ which we can rewrite as $q \mid p^{q-1} - 1$ and $p \mid q^{p-1} - 1$. Multiplying these together gives $pq \mid p^{q-1}q^{p-1} - p^{q+1} - q^{p-1} + 1$. Since $pq \mid p^{q-1}q^{p-1}$, we get that $pq \mid p^{q-1} + q^{p-1} - 1$ which we can rewrite as $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$. \square

A4) A deck of cards is shuffled by cutting the deck into two piles of 26 cards. Then, the new deck is formed by alternating cards from the two piles, starting with the bottom pile.

a) Show that if a card begins in the k -th position in the deck, it will be in the d -th position in the new deck, where $d \equiv 2k \pmod{53}$ and $1 \leq d \leq 52$.

Proof. This can easily be verified by checking the 52 cases individually. \square

b) Determine the number of shuffles of the type described above that are needed to return the deck of cards to its original order.

Proof. We are interested in finding an n such that $2^n k \equiv k \pmod{53}$ or equivalently, $2^n \equiv 1 \pmod{53}$. By Fermat's Theorem $2^{52} \equiv 1 \pmod{53}$ and so $n = 52$ is a valid number of shuffles that will restore the deck to its original order. \square

Extra Credit Problems.

EC1) Show that every odd prime except 5 divides some number of the form $111 \dots 11$ (k digits, all ones).

Proof. For the case of $p = 3$, we have that $3 \mid 111$. For $p > 5$, note that $p \mid 10^{p-1} - 1$ by Fermat's Theorem. $10^{p-1} - 1 = 999 \dots 999$ where there are $p - 1$ 9's. Since $(3, p) = 1$ we get that $p \mid 111 \dots 111$ where there are $p - 1$ 1's. □

EC2) A *complete system of residues modulo n* is a set of n numbers such that no two of them are congruent modulo n . Let p be an odd prime and let a_1, \dots, a_p and b_1, \dots, b_p be complete systems of residues modulo p . Prove that $a_1 b_1, \dots, a_p b_p$ is not a complete system of residues modulo p .

Proof. □