MATH 324 Summer 2006
Elementary Number Theory
Solutions to Assignment 4
Due: Thursday August 10, 2006

Department of Mathematical and Statistical Sciences
University of Alberta

Question 1. [p 221. #14]

Using Fermat's little theorem, find the last digit of the base 7 expansion of 3^{100}.

SOLUTION: From Fermat's little theorem, since 7 is prime, we have

$$3^6 \equiv 1 \pmod 7$$

so that

$$3^{100} \equiv \left(3^6\right)^{16} \cdot 3^4 \equiv \left(3^2\right)^2 \equiv 2^2 \equiv 4 \pmod 7,$$

so the last digit of the base 7 expansion of 3^{100} is 4.

Question 2. [p 221. #23]

Show that

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$$

whenever p is prime. (It has been conjectured that the converse of this is also true.)

SOLUTION: Since p is prime and $(k, p) = 1$ for $1 \leq k \leq p-1$, then Fermat's little theorem implies that

$$k^{p-1} \equiv 1 \pmod p$$

for $1 \leq k \leq p-1$, and therefore

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

Question 3. [p 222. #28]

Show that if p and q are distinct primes, then

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

SOLUTION: By Fermat's little theorem, since q is prime and $q \nmid p$, then

$$p^{q-1} \equiv 1 \pmod q,$$

so that $p^{q-1} = 1 + k \cdot q$ for some integer k, that is,

$$q \mid p^{q-1} + q^{p-1} - 1.$$

Similarly,

$$p \mid p^{q-1} + q^{p-1} - 1.$$

Therefore,

$$[p, q] \mid p^{q-1} + q^{p-1} - 1,$$

but $[p, q] = p \cdot q$, so that

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

Question 4. [p 222. #39]

(a) Show that if p is a prime, then $\binom{2p}{p} \equiv 2 \pmod{p^2}$.

(b) Can you show that if p is prime, then $\binom{2p}{p} \equiv 2 \pmod{p^3}$?

SOLUTION:

(a) Suppose that p is a prime, from the binomial theorem,

$$(1+x)^{2p} = \sum_{k=0}^{2p} \binom{2p}{k} x^k,$$

and the coefficient of x^p in this expansion is $\binom{2p}{p}$.

Also,

$$(1+x)^{2p} = (1+x)^p (1+x)^p = \left[\binom{p}{0} + \binom{p}{1}x + \cdots + \binom{p}{p}x^p\right]\left[\binom{p}{0} + \binom{p}{1}x + \cdots + \binom{p}{p}x^p\right],$$

and the coefficient of x^p is

$$\binom{p}{0}\binom{p}{p} + \binom{p}{1}\binom{p}{p-1} + \binom{p}{2}\binom{p}{p-2} + \cdots + \binom{p}{p-1}\binom{p}{1} + \binom{p}{p}\binom{p}{0},$$

that is,

$$\binom{2p}{p} = \sum_{k=0}^{p} \binom{p}{k}\binom{p}{p-k} = \sum_{k=0}^{p} \binom{p}{k}^2,$$

so that

$$\binom{2p}{p} = 2 + \sum_{k=1}^{p-1} \binom{p}{k}^2,$$

and since $p \left| \binom{p}{k} \right.$ for $1 \le k \le p-1$, then $p^2 \left| \binom{2p}{p} - 2 \right.$, that is,

$$\binom{2p}{p} \equiv 2 \pmod{p^2}.$$

(b) In *Mathematische Intelligencer* **10** (1988), # 3, page 42, it is shown that if $p > 3$ is a prime, then

$$\binom{2p-1}{p} \equiv 1 \pmod{p^3}. \qquad (*)$$

The proof of $(*)$ uses

Wolstenholme's Theorem: If p is a prime with $p \ge 5$, then

$$(p-1)!\left\{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}\right\} \equiv 0 \pmod{p^2}.$$

Using Wolstenholme's congruence, we can, in fact, prove that if p is a prime with $p \geq 5$, and m is any positive integer, then

$$\binom{mp-1}{p-1} \equiv 1 \pmod{p^3}. \qquad (**)$$

Note that $(**)$ reduces to $(*)$ for $m = 2$.

Now,

$$\binom{2p}{p} = \frac{(2p)!}{p!\,p!} = 2\frac{(2p-1)!}{p!\,(p-1)!} = 2\binom{2p-1}{p},$$

and from $(*)$ we have

$$\binom{2p}{p} \equiv 2\binom{2p-1}{p} \equiv 2 \cdot 1 \equiv 2 \pmod{p^3}.$$

Question 5. [p 222. #46]

Show that if n is a positive integer with $n \geq 2$, then n does not divide $2^n - 1$.

SOLUTION: Suppose to the contrary, that $n \geq 2$ and $n \mid 2^n - 1$. Let p be the smallest prime divisor of n and let δ be the smallest positive integer such that $p \mid 2^\delta - 1$ (δ exists, since $p \mid n$ and $n \mid 2^n - 1$ implies that $p \mid 2^n - 1$, now use the well–ordering property).

Now, since $p > 1$, then we must have $\delta > 1$. Next we note that $p \mid 2^n - 1$ implies that $\delta \mid n$. To see that this is the case, suppose that $n = \delta \cdot k + r$, where $0 < r < \delta$, then $2^n - 1 = 2^{k\cdot\delta} \cdot 2^r - 1$, and since $p \mid 2^\delta - 1$ implies that $2^\delta \equiv 1 \pmod{p}$, then $2^n - 1 \equiv 2^r - 1 \pmod{p}$. But $p \mid 2^n - 1$ implies that $p \mid 2^r - 1$ with $0 < r < \delta$, and this contradicts the choice of δ. Therefore, $\delta \mid n$.

By Fermat's little theorem, $p \mid 2^{p-1} - 1$, and this implies (from the definition of δ) that $\delta \leq p - 1$. Therefore, $1 < \delta < p$ and $\delta \mid n$. But then δ has a prime divisor which is less than p, and which divides n. However, this contradicts the definition of p.

Therefore, if n is a positive integer with $n \geq 2$, then $n \nmid 2^n - 1$.

Question 6. [p 236. #2]

Find a reduced residue system modulo 2^m, where m is a positive integer.

SOLUTION: First note that

$$\phi(2^m) = 2^{m-1}(2-1) = 2^{m-1}$$

and for $1 \leq k \leq 2^m$, only the odd integers are relatively prime to 2^m. There are 2^{m-1} of them, and no two of them are congruent modulo 2^m.

Therefore, the set of odd integers

$$1,\ 3,\ 5,\ \ldots,\ 2^m - 1$$

form a reduced residue system modulo 2^m.

Question 7. [p 236. #6]

Find the last digit of the decimal expansion of $7^{999,999}$.

SOLUTION: We have

$$\begin{aligned} 7^2 &\equiv 9 \pmod{10} \\ 7^3 &\equiv 3 \pmod{10} \\ 7^4 &\equiv 1 \pmod{10} \end{aligned}$$

and $999,999 = 299,999 \cdot 4 + 1$, so that

$$7^{999,999} \equiv \left(7^4\right)^{299,999} \cdot 7^1 \equiv 7 \pmod{10},$$

and the last digit of $7^{999,999}$ is a 7.

Question 8. [p 236. #10]

Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ if a and b are relatively prime positive integers.

SOLUTION: If $(a, b) = 1$, from Euler's theorem,

$$a^{\phi(b)} \equiv 1 \pmod{b},$$

so

$$a^{\phi(b)} = 1 + k \cdot b$$

for some integer k, so that

$$b \mid a^{\phi(b)} + b^{\phi(a)} - 1.$$

Similarly,

$$a \mid a^{\phi(b)} + b^{\phi(a)} - 1.$$

Therefore,

$$[a, b] \mid a^{\phi(b)} + b^{\phi(a)} - 1,$$

and since $(a, b) = 1$, then $[a, b] = ab$, so that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}.$$

Question 9. [p 236. #20]

Show that if m is a positive integer, $m > 1$, then $a^m \equiv a^{m-\phi(m)} \pmod{m}$ for all positive integers a.

SOLUTION: Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the canonical prime power factorization of m, then

$$\phi(m) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

Note that $p_i^{\alpha_i - 1}(p_i - 1) = \phi(p_i^{\alpha_i}) \mid \phi(m)$ for $i = 1, 2, \ldots, k$.

(a) If $(a, p_i) = 1$, then $(a, p_i^{\alpha_i}) = 1$, and from Euler's theorem we have $p_i^{\alpha_i} \mid a^{\phi(p_i^{\alpha_i})} - 1$, and since $\phi(p_i^{\alpha_i}) \mid \phi(m)$, then $p_i^{\alpha_i} \mid a^{\phi(m)} - 1$
(use the fact that

$$a^{r \cdot s} - 1 = \left(a^r\right)^s - 1 = \left(a^r - 1\right)\left((a^r)^{s-1} + (a^r)^{s-2} + \cdots + a^r + 1\right)$$

for positive integers r and s). Therefore, if $(a, p_i) = 1$, then $p_i^{\alpha_i} \mid a^{\phi(m)} - 1$.

(b) Now, if α and $p \geq 2$ are positive integers, then $p^{\alpha-1} \geq \alpha$ (prove this by induction). However, for $i = 1, 2, \ldots, k$, we have $p_i^{\alpha_i - 1} \mid m$ and $p_i^{\alpha_i - 1} \mid \phi(m)$, so that $p_i^{\alpha_i - 1} \mid m - \phi(m)$. Also, $m - \phi(m) > 0$ for $m > 1$, so that $m - \phi(m) \geq p_i^{\alpha_i - 1} \geq \alpha_i$ for $i = 1, 2, \ldots, k$. If $(a, p_i) > 1$, that is, if $p_i \mid a$, then $p_i^{\alpha_i} \mid p_i^{m-\phi(m)}$ and $p_i^{m-\phi(m)} \mid a^{m-\phi(m)}$, therefore, $p_i^{\alpha_i} \mid a^{m-\phi(m)}$.

(c) So that for *any* positive integer a we have $p_i^{\alpha_i} \mid a^{m-\phi(m)}(a^{\phi(m)} - 1)$ for $i = 1, 2, \ldots, k$. Therefore, $a^m \equiv a^{m-\phi(m)} \pmod{m}$ for all positive integers a.

Question 10. [p 246. #14]

For which positive integers n does $\phi(n) \mid n$?

SOLUTION: Suppose that n is a positive integer and let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

be the prime power decomposition of n, then

$$\phi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

If $\phi(n) \mid n$, then

$$\frac{p_1}{p_1 - 1} \cdot \frac{p_2}{p_2 - 1} \cdots \frac{p_k}{p_k - 1} \qquad (\dagger)$$

is a positive integer, and since the numerator can have at most one factor of 2, this implies that the denominator can contain at most one factor $(p_i - 1)$ where p_i is an odd prime.

Therefore, in the prime power decomposition of n, either $n = 2^\alpha$ or $n = 2^\alpha p^\beta$, where p is an odd prime, and $\alpha \geq 0$ and $\beta \geq 0$.

case (i): If $n = 2^\alpha$ where $\alpha \geq 0$, then for $\alpha = 0$, we have $n = 1$ and $\phi(n) = 1$, while for $\alpha \geq 1$, we have $n = 2^\alpha$ and $\phi(n) = 2^{\alpha-1}(2 - 1) = 2^{\alpha-1} = \dfrac{n}{2}$.

case (ii): If $n = 2^\alpha p^\beta$, where p is an odd prime, and $\beta \geq 1$, then

$$\phi(n) = n \cdot \frac{2 - 1}{2} \cdot \frac{p - 1}{p}$$

and since $\phi(n) \mid n$, then

$$k = \frac{n}{\phi(n)} = \frac{2p}{p - 1}$$

is an integer, so that $p - 1 = 2$, that is, $p = 3$, and $n = 2^\alpha 3^\beta$ where $\alpha \geq 0$ and $\beta \geq 1$.

Therefore, the only positive integers n for which $\phi(n) \mid n$ are given by

$$n = 1, \quad 2^\alpha, \quad 2^\alpha\, 3^\beta$$

where α, $\beta \geq 1$.