Math 324**, Fall** 2011
Assignment 5
Solutions

Exercise 1. (a) Find the least positive residue of $2^{1000000}$ modulo 17.
(b) Find the least positive residue of 3^{1000} modulo 42.
Solutions : (a) Observing that 17 is prime, Fermat's Little Theorem asserts that

$$a^{16} \equiv 1 \bmod 17$$

for all integers a with $\gcd(a, 17) = 1$. Observing that

$$1000000 = 16 \cdot 62500$$

the fact 2 and 17 are relatively prime allows us to conclude

$$2^{1000000} = \left(2^{16}\right)^{62500} \equiv 1^{62500} = 1 \bmod 17.$$

Therefore, 1 is the least positive residue of $2^{1000000}$ modulo 17.
(b) We first observe that

$$42 = 2 \cdot 3 \cdot 7.$$

We note that

$$3^{1000} \equiv 0 \bmod 3.$$

while

$$3^{1000} \equiv 1^{1000} = 1 \bmod 2.$$

Since $\phi(7) = 6$ and

$$1000 = 166 \cdot 6 + 4,$$

Fermat's Little Theorem yields

$$3^{1000} = \left(3^6\right)^{166} \cdot 3^4 \equiv 1^{166} \cdot 3^4 = 81 \equiv 4 \bmod 7.$$

In light of the above discussion, the least positive residue x of 3^{1000} is a solution of the system of congruences

$$\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 0 \bmod 3 \\ x &\equiv 4 \bmod 7 \end{aligned} \tag{1}$$

By inspection, the first two equations of (1) have the solution

$$x \equiv 3 \bmod 6.$$

Thus (1) is equivalent to

$$\begin{aligned} x &\equiv 3 \bmod 6 \\ x &\equiv 4 \bmod 7 \end{aligned}$$

Observing

$$1 = 7 - 6,$$

we deduce that

$$x = 3 \cdot 7 - 4 \cdot 6 = 21 - 24 = -3 \equiv 39 \bmod 42.$$

Exercise 2. Use Euler's Theorem to solve the following congruences.

(i) $4x \equiv 11 \bmod 19$.
(ii) $8x \equiv 13 \bmod 22$.

Solution : (a) Observing $\gcd(4,19) = 1$ and $\phi(19) = 18$ (since 19 is prime), Euler's Theorem asserts that

$$4^{18} \equiv 1 \bmod 19.$$

Therefore,

$$x \equiv 4^{18}x = 4^{17} \cdot 4x \equiv 4^{17} \cdot 11 \bmod 19$$

This can be further simplified by observing

$$4^{17} = \left(2^2\right)^{17} = 2^{34} = 2^{18} \cdot 2^{16} \equiv 2^{16} \bmod 19.$$

Since

$$2^4 = 16 \equiv -3 \bmod 19 \qquad \text{and} \qquad 3^4 = 81 \equiv 5 \bmod 19,$$

we have

$$4^{17} \equiv 2^{16} = \left(2^4\right)^4 \equiv (-3)^4 \equiv 5 \bmod 19,$$

hence

$$x \equiv 4^{17} \cdot 11 \equiv 5 \cdot 11 = 55 \equiv 17 \equiv -2 \bmod 19.$$

In summary, the congruence

$$4x \equiv 11 \bmod 19$$

has the solution

$$x \equiv -2 \bmod 19.$$

(b) Observing $\gcd(8,22) = 2$ does not divide 13, the congruence

$$8x \equiv 13 \bmod 22$$

has no solution.

Exercise 3. (a) Let n be an odd integer. If $3 \not| n$, show $n^2 \equiv 1 \bmod 24$.
(b) Show that $a^6 - 1$ is divisible by 168 whenever $\gcd(a,42) = 1$.

Solution : (a) Writing $n = 2l + 1$, we have

$$n^2 = (2l+1) = 4l^2 + 4l + 1 = 4l(l+1) + 1.$$

Since one of l or $l+1$ is even, $4l(l+1)$ is divisible by 8, henc

$$n^2 \equiv 1 \bmod 8. \tag{1}$$

Since 3 is prime, if 3 does not divide n then $\gcd(3,n) = 1$. Observing $\phi(3) = 2$, Euler's Theorem allows us to deduce

$$n^2 \equiv 1 \bmod 3. \tag{2}$$

In light of (1) and (2), the fact $\gcd(3,8) = 1$ allows us to conclude that

$$n^2 \equiv 1 \bmod 3 \cdot 8 = 24.$$

(b) We first observe

$$168 = 8 \cdot 3 \cdot 7.$$

If $\gcd(a,42) = 1$ then

$$\gcd(a,2) = \gcd(a,3) = \gcd(a,7) = 1.$$

In particular, a is odd and 3 does not divide n, so part (a) shows

$$a^2 \equiv 1 \bmod 24.$$

Afortiori,

$$a^6 = (a^2)^3 \equiv 1^3 = 1 \bmod 24. \tag{1}$$

On the other hand, since $\gcd(a, 7) = 1$ and $\phi(7) = 6$, Euler's Theorem yields

$$a^6 = 1 \bmod 7. \tag{2}$$

Finally, since $\gcd(24, 7) = 1$, equations (1) and (2) allow us to conclude

$$a^6 \equiv 1 \bmod 7 \cdot 24 = 168,$$

i.e. $a^6 - 1$ is divisible by 168.

Exercise 4.(a) Let p and q be distinct primes. Show

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

(b) Let p be an odd prime. Show

$$1^2 \cdot 3^2 \cdots (p-4)^2(p-2)^2 \equiv (-1)^{(p+1)/2} \bmod p.$$

Solution : (a) Since p and q are distinct primes, $\gcd(p, q) = 1$. Recognizing $q \geq 2$, Fermat's Little Theorem yeilds

$$p^{q-1} + q^{p-1} \equiv 0 + 1 = 1 \bmod p.$$

Similarly,

$$p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \bmod q.$$

The fact $\gcd(p, q) = 1$ allows us to conclude

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

(b) By Wilson's Theorem,

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv -1 \bmod p. \tag{1}$$

By grouping odd and even factors, the product on the left can be rewritten as

$$\prod_{j=1}^{(p-1)/2} 2j - 1 \cdot \prod_{j=1}^{(p-1)/2} 2j.$$

Consider the second product. Since

$$2j \equiv 2j - p = -(p - 2j),$$

we have

$$\prod_{j=1}^{(p-1)/2} 2j \equiv \prod_{j=1}^{(p-1)/2} -(p-2j) \equiv (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (p-2j) \bmod p.$$

As j increases from 1 to $(p-1)/2$ in steps of 1, $p - 2j$ decreases from $p - 2$ to 1 in steps of 2. It follows that

$$\prod_{j=1}^{(p-1)/2} (p-2j) = \prod_{j=1}^{(p-1)/2} 2j - 1.$$

Putting this all together, we deduce

$$\prod_{j=1}^{(p-1)/2} 2j-1 \cdot \prod_{j=1}^{(p-1)/2} 2j \equiv \prod_{j=1}^{(p-1)/2} 2j-1 \cdot (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} 2j-1 = (-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (2j-1)^2 \bmod p.$$

Subsituting in (1), we conclude

$$(-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (2j-1)^2 \equiv -1 \bmod p.$$

Since $p-1$ is even, multiplication by $(-1)^{(p-1)/2}$ yields

$$\prod_{j=1}^{(p-1)/2} (2j-1)^2 \equiv (-1)^{(p+1)/2} \bmod p.$$

Exercise 5. (a) Let a and m be positive integers with

$$\gcd(a,m) = \gcd(a-1,m) = 1.$$

Show

$$1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \bmod m.$$

Solution : Since $\gcd(a,m) = 1$, Euler's Theorem asserts

$$a^{\phi(m)} - 1 \equiv 0 \bmod m.$$

On the other hand, since $\phi(m) > 0$, we have

$$a^{\phi(m)} - 1 = (a-1)(a^{\phi(m)-1} + \cdots + 1),$$

hence

$$(a-1)(a^{\phi(m)-1} + \cdots + 1) \equiv 0 \bmod m.$$

Since $\gcd(a-1,m) = 1$, $a-1$ is invertible modulo m. Multiplying the last equation by an inverse of $a-1$ modulo m, we deduce

$$a^{\phi(m)-1} + \cdots + 1 \equiv 0 \bmod m,$$

as required.

Exercise 6. Let m_1, m_2, ..., m_r be a set of pairwise relatively prime integers. Set

$$M = m_1 \cdots m_r, \qquad M_j = \frac{M}{m_j}, 1 \le j \le r.$$

Show that the solution of the system of congruences

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

is

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_r M_r^{\phi(m_r)} \bmod M.$$

Solution : The Chinese Remainder Theorem asserts that the given system of congruences has a unique solution modulo M. Therefore, it is sufficient to verify that

$$x = a_1 M_1^{\phi(m_1)} + \cdots + a_r M_r^{\phi(m_r)}$$

is a solution of the system.

Given j, $1 \leq j \leq r$, we have

$$\gcd(m_j, M_j) = 1.$$

Therefore, Euler's Theorem asserts

$$M_j^{\phi(m_j)} \equiv 1 \bmod m_j.$$

On the other hand, if $i \neq j$ then m_j divides M_i. Observing $\phi(m_i) > 0$, we conclude

$$M_i^{\phi(m_i)} \equiv 0 \bmod m_j.$$

Therefore,

$$x = \sum_{i=1}^{r} a_i M_i^{\phi(m_i)} \equiv a_j M_j^{\phi(m_j)} \equiv a_j \cdot 1 = a_j \bmod m_j.$$

Since j was essentially arbitrary, x is a solution of the given system, as required.

Exercise 7. (a) Let a and n be relatively prime positive integers. Show that if n is a pseudoprime to the base a then n is a pseudoprime to the base $\bar{a}$, where $\bar{a}$ is an inverse of a modulo n.
(b) Show that every integer of the form

$$(6m+1)(12m+1)(18m+1)$$

where m is a positive integer such that $6m+1$, $12m+1$, and $18m+1$ are all prime is a Carmichael number.
Solution : (a) By hypothesis,

$$a^{n-1} \equiv 1 \bmod n.$$

Multiplying by $\bar{a}^{n-1}$, we deduce

$$\bar{a}^{n-1} \equiv \bar{a}^{n-1} a^{n-1} = (\bar{a} \cdot a)^{n-1} \equiv 1^{n-1} = 1 \bmod n.$$

Since n is composite (being a pseudoprime) and $\gcd(\bar{a}, n) = 1$ ($\bar{a}$ is invertible modulo n), this shows that n is a pseudoprime to the base $\bar{a}$.
(b) Setting

$$n = (6m+1)(12m+1)(18m+1)$$

we calculate

$$n = (72m^2 + 18m + 1)(18m+1) = 1296m^3 + 396m^2 + 36m + 1.$$

Therefore,

$$n - 1 = 1296m^3 + 396m^2 + 36m = 18m(72m^2 + 22m + 2) = 12m(108m^2 + 33m + 3).$$

It follows immediately that $n-1$ is divisible by $6m+1-1 = 6m$, $12m+1-1 = 12m$, and $18m+1-1 = 18m$. Since $6m+1$, $12m+1$ and $18m+1$ are clearly disitinct, if they are each prime then the characterization of Carmichael numbers proved in class allows us to deduce that n is a Carmichael number.

Bonus Question. Let p be prime and let a be a positive integer not divisible by p. The *Fermat quotient* $q_p(a)$ of a is defined by

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

Show that if a and b are positive integers with $\gcd(p, ab) = 1$ then

$$q_p(ab) \equiv q_p(a) + q_p(b) \bmod p.$$

Solution : By definition,

$$a^{p-1} = 1 + pq_p(a)$$

Therefore,

$$(ab)^{p-1} = a^{p-1}b^{p-1} = (1 + pq_p(a))(1 + pq_p(b)) = 1 + p[q_p(a) + q_p(b) + pq_p(a)q_p(b)].$$

Hence

$$q_p(ab) = q_p(a) + q_p(b) + pq_p(a)q_p(b) \equiv q_p(a) + q_p(b) \bmod p.$$