Homework 5 Solutions

#9.2

(a) Try computing it for some primes, say $p \leq 13$. The pattern quickly becomes clear.

(b) We actually did this in class a bit before the homework was due, as it is a bit clever.

But the idea is to pair up the numbers $1, 2, \ldots, p-1$ so that their product is congruent to $1 \bmod p$. We know for each n in $1, 2, \ldots, p-1$ that

$$nx \equiv 1 \pmod{p}$$

has a solution, as $\gcd(n,p)=1$. But when is

$$x^2 \equiv 1 \pmod{p} \; ?$$

If $x^2 \equiv 1 \; (p)$, then $p \mid x^2-1 = (x+1)(x-1)$, and so $p \mid (x+1)$ or $p \mid (x-1)$. Thus either $x \equiv 1 \; (p)$ or $x \equiv -1 \; (p)$.

This means that for all other numbers besides 1 and $p-1$, they pair up. But $1, -1$ don't pair up.

So $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 1 \cdot 1 \cdot \cdots \cdot 1 \cdot (p-1) \equiv -1 \; (p)$.

10.1 This is similar in spirit to 9.2.

For each b in $b_1, b_2, \dots, b_{\phi(m)}$, there is a solution x to $bx \equiv 1 \pmod m$, as $\gcd(b,m)=1$. Further, we know this solution is unique mod m.

There are 2 cases. If b and x are different, then we can cancel them as they both appear in B. Otherwise, $b \equiv x$, and $b^2 \equiv 1 \pmod m$.

So $B \equiv (c_1)^{*} (c_2)^{*} \cdots (c_k)^{*} \pmod m$, where c_i denote those b satisfying $c_i^2 \equiv 1 \pmod m$.

Now we need a new idea, and there are multiple approaches. One good approach is to now consider the congruences $cx \equiv -1 \pmod m$. As $\gcd(c,m)=1$, this has a solution too. Squaring, we see that

$$c^2 x^2 \equiv 1 \mod m.$$

As $c^2 \equiv 1 \pmod m$, this becomes $x^2 \equiv 1 \pmod m$, & so x is one of the c's!

So the c values pair up to give (-1)'s, & B will be 1 if there are an even number of pairs of c, & -1 if there are an odd number of pairs.

∎

10.2 By Euler's formula, as $\varphi(1000) = 1$ and $\gcd(7, 3750) = 1$, we have $7^{1000} \equiv 1 \pmod{3750}$.

So $7^{3003} \equiv (7^{1000})^3 7^3 \equiv 7^3 \equiv 343 \pmod{3750}$, which is almost our answer. But $7 \mid 343$.

So we add 3750 (as $343 \equiv 343 + 3750 \pmod{3750}$), and get the answer 4093. ∎

10.3 $n = 561 = 3 \cdot 11 \cdot 17$.

Take a with $\gcd(a, 561) = 1$. Then by FLT, we have

$$\begin{cases} a^2 \equiv 1 \pmod{3} \\ a^{10} \equiv 1 \pmod{11} \\ a^{16} \equiv 1 \pmod{17} \end{cases}$$

As 2, 10, 16 all divide $561 - 1 = 560$, we have

$$\begin{cases} a^{560} \equiv 1 \pmod{3} \\ a^{560} \equiv 1 \pmod{11} \\ a^{560} \equiv 1 \pmod{17} \end{cases}$$

And so $3 \mid a^{560} - 1$, $11 \mid a^{560} - 1$, $17 \mid a^{560} - 1$.

By Unique factorization, this means $3 \cdot 11 \cdot 17 \mid a^{560} - 1$, which is what we wanted to show. ∎

Note: there are infinitely many Carmichael numbers, & this is sort of a deep question.

11.2 (a) Write $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

If $p = 2$, then $\varphi(2^a) = 2^a - 2^{a-1}$, which is even unless $a = 1$.

If p is odd, then $\varphi(p^a) = p^a - p^{a-1}$, which is the difference of odd numbers & is thus even.

As φ is multiplicative, if any odd prime appears, or if $2^2 \mid m$, then $\varphi(m)$ is even. ∎

(b) Building on the above, if two distinct odd primes divide m, then $\varphi(m)$ is divisible by 4. Further, $\varphi(2^a)$ is divisible by 2 if $a = 2$, and divisible by 4 if $a \geq 3$.

So we only need to consider $m = p^a$, $2p^a$ (for a or 2 or 4), where p is an odd prime.

As $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$, we see that this is divisible by 2 always, & divisible by 4 exactly when $p \equiv 1 \pmod 4$.

So in total, $\varphi(m)$ is not divisible by 4 when $m = 1$, $m = 2$, $m = 4$, $m = p^a$, or $m = 2p^a$ for a prime $p \equiv 3 \pmod 4$. ∎

11.3 We know $\varphi(m) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$

$$= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right)$$

$$= m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

So $\varphi(1000000) = 1000000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000000 \cdot \frac{4}{10} = 400000.$ ∎

11.5 a) $\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 5 \pmod 9 \end{cases} \Rightarrow x = 3+7m$

$\Rightarrow 3+7m \equiv 5 \bmod 9$

$7m \equiv 2 \bmod 9$

So $m \equiv -1 \bmod 9$,

i.e. $m = -1 + 9k$.

And so $x = 3+7m = 3+7(-1+9k) = -4+27k$,

meaning $x \equiv -4 \equiv 23 \bmod 27$. ∎

b) $\begin{cases} x \equiv 3 \pmod{37} \\ x \equiv 1 \pmod{87} \end{cases}$

$x = 3+37m \equiv 1 \bmod 87$

$37m \equiv 85 \bmod 87$.

$37m \equiv -2 \bmod 87$.

By the Euclidean Algorithm (which I used at right), we see $m \equiv 7 \bmod 87$.

So $x = 3+37m = 3+37(7+87k)$

$= 262 + 37\cdot 87k$.

And $x \equiv 262 \bmod (37\cdot 87)$. ∎

Eucl. Alg:

$87 = 2\cdot 37 + 13$

$37 = 2\cdot 13 + 11$

$13 = 1\cdot 11 + 2$

$11 = 5\cdot 2 + 1$

$\Rightarrow 1 = 11 - 2\cdot 5 = 11 - 5(13-11)$

$= 6\cdot 11 - 5\cdot 13 = 6\cdot(37-2\cdot 13) - 5\cdot 13$

$= 6\cdot 37 - 17\cdot 13$

$= 6\cdot 37 - 17(87-2\cdot 37)$

$= 37\cdot 40 - 17\cdot 87$.

So $37\cdot 40 \equiv 1 \bmod 87$,

+ $37\cdot(-80) \equiv -2 \bmod 87$,

$-80 \equiv 7 \bmod 87$.

c) $\begin{cases} x \equiv 5 \ (7) \\ x \equiv 2 \ (12) \\ x \equiv 8 \ (13) \end{cases}$

Begin with $\begin{cases} x \equiv 5 \ (7) \\ x \equiv 2 \ (12) \end{cases}$.

$x = 5 + 7m \equiv 2 \mod 12$,

So $7m \equiv -3 \mod 12$.

$\Longrightarrow m \equiv 3 \mod 12$,

So $x = 5 + 7(3 + 12k) = 5 + 21 + 7 \cdot 12k$

$= 26 + 7 \cdot 12k \equiv 26 \mod (7 \cdot 12)$.

Now we have the pair

$\begin{cases} x \equiv 26 \mod (7 \cdot 12) \\ x \equiv 8 \mod (13) \end{cases}$.

$x = 26 + 7 \cdot 12m \equiv 8 \mod 13$

$\Longrightarrow 7 \cdot 12m \equiv 8 \mod 13$

$\Longrightarrow -7m \equiv 8 \mod 13$

$\Longrightarrow 7m \equiv 5 \mod 13$

$\Longrightarrow m \equiv -3 \mod 13$.

So $x = 26 + 7 \cdot 12(-3 + 13k)$

$x = 26 + -3 \cdot 7 \cdot 12 + 7 \cdot 12 \cdot 13k$

or $x \equiv 26 - 3 \cdot 7 \cdot 12 \mod (7 \cdot 12 \cdot 13)$

all the same.

$\begin{cases} (\text{or} \quad x \equiv -226 \mod (7 \cdot 12 \cdot 13)) \\ (\text{or} \quad x \equiv 866 \mod 1092). \end{cases}$