Homework 3

Rebekah Mayne
Math 370, Fall 2024

February 24, 2025

1 (Page 40)

Problem 7. Solve $9x \equiv 4 \pmod{1453}$.

Solution.
We can look for solutions by doing the following

$$9 \overset{?}{\mid} 1453 + 4 \to (1 + 4 + 5 + 7 \equiv 8 \pmod 9) \to 9 \nmid 1457$$
$$9 \overset{?}{\mid} 1457 + 1453 \to (2 + 9 + 1 + 0 \equiv 3 \pmod 9) \to 9 \nmid 2910$$
$$9 \overset{?}{\mid} 2910 + 1453 \to (4 + 3 + 6 + 3 \equiv 7 \pmod 9) \to 9 \nmid 4363$$
$$9 \overset{?}{\mid} 4363 + 1453 \to (5 + 8 + 1 + 6 \equiv 2 \pmod 9) \to 9 \nmid 5816$$
$$9 \overset{?}{\mid} 5816 + 1453 \to (7 + 2 + 6 + 9 \equiv 6 \pmod 9) \to 9 \nmid 7269$$
$$9 \overset{?}{\mid} 7269 + 1453 \to (8 + 7 + 2 + 2 \equiv 1 \pmod 9) \to 9 \nmid 8722$$
$$9 \overset{?}{\mid} 8722 + 1453 \to (1 + 0 + 1 + 7 + 5 \equiv 5 \pmod 9) \to 9 \nmid 10175$$
$$9 \overset{?}{\mid} 10175 + 1453 \to (1 + 1 + 6 + 2 + 8 \equiv 0 \pmod 9) \to 9|11628$$

Then, we can see that $9(1282) = 11628 \equiv 4 \pmod{1453}$. So $x \equiv 1282 \pmod{1453}$.

Problem 8. Solve $4x \equiv 9 \pmod{1453}$.

Solution.
We can look for solutions by doing the following (after the first, we can only check even multiples of 1453, because it has to be even to be divisible.)

$$4 \overset{?}{\mid} 1453 + 9 \to (4 \nmid 62) \to 4 \nmid 1462$$
$$4 \overset{?}{\mid} 2915 + 1453(2) \to (4|68) \to 4|4368$$

Then, we can see that $4(1092) = 4368 \equiv 9 \pmod{1453}$. So $x \equiv 1092 \pmod{1453}$.

Problem 15. Find a positive integer such that half of it is a square, a third of it is a cube, and a fifth of it is a fifth power.

Solution.

Let n be a positive integer. Then we want $a^2 = \frac{n}{2}$, $b^3 = \frac{n}{3}$ and $c^5 = \frac{n}{5}$. Or rewritten as $n = 2a^2$, $n = 3b^3$, and $n = 5c^5$. Then we know that $3, 2, 5 | n$ So we need to be able to find $i_1, i_2, i_3, j_1, j_2, j_3, k_1, k_2, k_3$ so that

$$n \quad = \quad (2^{2i_1+1})(3^{2j_1})(5^{2k_1}) \quad = \quad (2^{3i_2})(3^{3j_2+1})(5^{3k_2}) \quad = \quad (2^{5i_3})(3^{5j_3})(5^{5k_3+1})$$

So we need to find $2i_1 + 1 = 3i_2 = 5i_3$, $2j_1 = 3j_2 + 1 = 5j_3$ and $2k_1 = 3k_2 = 5k_3 + 1$.

For the first, we can see that for $2i_1 + 1 = 3i_2 = 5i_3 = e_1$, this means that $2i_1 + 1$ must be divisible by 3 and 5. So let $e_1 = 2i_1 + 1 \equiv 0 \pmod 3$ and $e_1 \equiv 0 \pmod 5$. Then,

$$\begin{array}{lll}
2i_1 + 1 \equiv 0 \pmod 3 & & \\
2i_1 \equiv -1 \pmod 3 & & \\
2i_1 \equiv 2 \pmod 3 & & \\
i_1 \equiv 1 \pmod 3 & \rightarrow & i_1 = 3r_1 + 1 \\
& & e_1 = 2(3r_1 + 1) + 1 \\
& & e_1 = 6r_1 + 3 \\
6r_1 + 3 \equiv 0 \pmod 5 & \leftarrow & \\
r_1 \equiv -3 \pmod 5 & & \\
r_1 \equiv 2 \pmod 5 & \rightarrow & r_1 = 5r_2 + 2 \\
& & e_1 = 6r_1 + 3 \\
& & e_1 = 6(5r_2 + 2) + 3 \\
& & e_1 = 30r_2 + 15 \\
e_1 \equiv 15 \pmod{30} & \leftarrow &
\end{array}$$

Then, we can let $e_1 = 45$. Then we want to find $e_2 = 2j_1 = 3j_2 + 1 = 5j_3$, this means that $e_2 = 3j_2 + 1 \equiv 0 \pmod 5$ and $e_2 \equiv 0 \pmod 2$. So

$$\begin{array}{lll}
3j_2 + 1 \equiv 0 \pmod 2 & & \\
j_2 \equiv -1 \pmod 2 & & \\
j_2 \equiv 1 \pmod 2 & \rightarrow & j_2 = 2r_1 + 1 \\
& & e_2 = 3(2r_1 + 1) + 1 \\
& & e_2 = 6r_1 + 4 \\
6r_1 + 4 \equiv 0 \pmod 5 & \leftarrow & \\
r_1 - 1 \equiv 0 \pmod 5 & & \\
r_1 \equiv 1 \pmod 5 & \rightarrow & r_1 = 5r_2 + 1 \\
& & e_2 = 6(5r_2 + 1) + 4 \\
& & e_2 = 30r_2 + 10 \\
e_2 \equiv 10 \pmod{30} & \leftarrow &
\end{array}$$

So lets let $e_2 = 40$. Then we want to find $e_3 = 2k_1 = 3k_2 = 5k_3 + 1$, this means that $e_3 = 5k_3 + 1 \equiv 0$

(mod 2) and $e_3 \equiv 0 \pmod 3$.

$$\begin{array}{lll}
5k_3 + 1 \equiv 0 \pmod 2 & & \\
k_3 \equiv -1 \pmod 2 & & \\
k_3 \equiv 1 \pmod 2 & \rightarrow & k_3 = 2r_1 + 1 \\
 & & e_2 = 5(2r_1+1)+1 \\
 & & e_2 = 10r_1 + 6 \\
10r_1 + 6 \equiv 0 \pmod 3 & \leftarrow & \\
r_1 \equiv 0 \pmod 3 & & \\
r_1 \equiv 0 \pmod 3 & \rightarrow & r_1 = 3r_2 + 1 \\
 & & e_2 = 10(3r_2+1)+6 \\
 & & e_2 = 30r_2 + 16 \\
e_2 \equiv 16 \pmod{30} & \leftarrow &
\end{array}$$

So lets let $e_2 = 36$. Then,

$$\begin{array}{lllllll}
(2^{45})(3^{40})(5^{36}) & = & (2^{2i_1+1})(3^{2j_1})(5^{2k_1}) & = & (2^{3i_2})(3^{3j_2+1})(5^{3k_2}) & = & (2^{5i_3})(3^{5j_3})(5^{5k_3+1}) \\
(2^{45})(3^{40})(5^{36}) & = & 2(2^{22}\cdot 3^{20}\cdot 5^{18})^2 & = & 3(2^{15}\cdot 3^{13}\cdot 5^{12})^3 & = & 5(2^{9}\cdot 3^{8}\cdot 5^{7})^5
\end{array}$$

So our $n = 2^{45}\cdot 3^{40}\cdot 5^{36}$.

Problem 16. The three consecutive integers 48,49, and 50 each have a square factor.

(a) Find n such that $3^2|n, 4^2|n+1$ and $5^2|n+2$.

(b) Can you find n such that $2^2|n, 3^2|n+1$ and $4^2|n+2$?

Solution.

(a) This can be rewritten as $n \equiv 0 \pmod{3^2}$, $n+1 \equiv 0 \pmod{4^2}$ and $n+2 \equiv 0 \pmod{5^2}$. Or $n \equiv 0 \pmod 9$, $n \equiv -1 \pmod{16}$ and $n \equiv -2 \pmod{25}$. Then, we can do the following to solve for n,

$$\begin{array}{lll}
n \equiv 0 \pmod 9 & \rightarrow & n = 9k_1 \\
9k_1 \equiv -1 \pmod{16} & \leftarrow & \\
*k_1 \equiv 7 \pmod{16} & \rightarrow & k_1 = 16k_2 + 7 \\
 & & n = 9(16k_2+7) \\
 & & n = 144k_2 + 63 \\
144k_2 + 63 \equiv -2 \pmod{25} & \leftarrow & \\
-6k_2 + 13 \equiv 23 \pmod{25} & & \\
-6k_2 \equiv 10 \pmod{25} & & \\
6k_2 \equiv 15 \pmod{25} & & \\
**\,k_2 \equiv 15 \pmod{25} & \rightarrow & k_2 = 25k_3 + 15 \\
 & & n = 144(25k_3+15)+63 \\
 & & n = 3600k_3 + 2160 + 63 \\
 & & n = 3600k_3 + 2223 \\
n \equiv 2223 \pmod{3600} & &
\end{array}$$

$*$ work:

k	0	1	2	3	4	5	6	7	$\cdots$
$9k \pmod{16}$	0	9	2	11	4	13	6	$15 \equiv -1$	$\cdots$

$**$ work:

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$6k \pmod{25}$	0	6	12	18	24	5	11	17	23	4	10	16	22

k	13	14	15	$\cdots$
$6k \pmod{25}$	3	9	15	$\cdots$

So let $n = 2223$, we can check that

$$\begin{aligned} 2223/3^2 &= 247 \checkmark \\ 2224/4^2 &= 139 \checkmark \\ 2225/5^2 &= 89 \checkmark \end{aligned}$$

(b) We know that $n \equiv 0 \pmod 4$, and that $16k = n + 2$ so we can check this out under mod 4

$$\begin{aligned} 16k &= n + 2 \\ 0 &\equiv 0 + 2 \pmod 4 \\ 0 &\equiv 2 \pmod 4 \end{aligned}$$

This is not possible, so we cannot find a solution.

2 (Page 48)

Problem 2. What is the least residue of

(a) $5^{10} \pmod{11}$

(b) $5^{12} \pmod{11}$

(c) $1945^{12} \pmod{11}$

Solution.

(a) By FLT, because $5 \perp 11$, and because 11 is prime, we know that $5^{10} \equiv 1 \pmod{11}$.

(b) $5^{12} \equiv 5 \cdot 5 \pmod{11}$ because 11 is prime, and $a^p \equiv a \pmod p$, so then

$$\begin{aligned} 5^{12} &\equiv 5 \cdot 5 \pmod{11} \\ &\equiv 25 \pmod{11} \\ 5^{12} &\equiv 3 \pmod{11} \end{aligned}$$

(c) By FLT, because $1945 \perp 11$, and because 11 is prime, we know that $1945^{10} \pmod{11} \equiv 1$, so we can see the following,

$$\begin{aligned}
1945^{12} &\equiv 1945^{10} \cdot 1945^2 &&\pmod{11}\\
&\equiv 1 \cdot 1945^2 &&\pmod{11}\\
&\equiv (1100 + 845)^2 &&\pmod{11}\\
&\equiv (770 + 75)^2 &&\pmod{11}\\
&\equiv (66 + 9)^2 &&\pmod{11}\\
&\equiv (9)^2 &&\pmod{11}\\
&\equiv (-2)^2 &&\pmod{11}\\
1945^{12} &\equiv 4 &&\pmod{11}
\end{aligned}$$

Problem 4. What are the last two digits of 7^{333}

Solution.

Look at $7^{333} \pmod{100}$. Or we can rewrite it using the Chinese remainder theory and solve for what $7^{333} \pmod{25}$ and $7^{333} \pmod{4}$ and combine. Starting we can see

$$\begin{aligned}
7^{333} &\equiv \left(7^2\right)^{166} \cdot 7 &&\pmod{25}\\
&\equiv (49)^{166} \cdot 7 &&\pmod{25}\\
&\equiv (-1)^{166} \cdot 7 &&\pmod{25}\\
7^{333} &\equiv 7 &&\pmod{25}
\end{aligned}$$

and

$$\begin{aligned}
7^{333} &\equiv (-1)^{333} &&\pmod{4}\\
&\equiv -1 &&\pmod{4}\\
7^{333} &\equiv 3 &&\pmod{4}
\end{aligned}$$

Then we want to solve for $x \equiv 3 \pmod{4}$ and $x \equiv 7 \pmod{25}$ as follows,

$$\begin{array}{lll}
x \equiv 3 \pmod{4} & \rightarrow & x = 4k_1 + 3\\
4k_1 + 3 \equiv 7 \pmod{25} & \leftarrow & \\
4k_1 \equiv 4 \pmod{25} & & \\
k_1 \equiv 1 \pmod{25} & \rightarrow & k_1 = 25k_2 + 1\\
 & & x = 4(25k_2 + 1) + 3\\
 & & x = 100k_2 + 4 + 3\\
 & & x = 100k_2 + 7\\
x \equiv 7 \pmod{100} & \leftarrow & \\
7^{333} \equiv 7 \pmod{100} & &
\end{array}$$

So we can see that the last two digits of 7^{333} is 07.

Problem 6. What is the remainder when 314^{162} is divided by 163?

Solution.

This can be rewritten as $314^{162} \pmod{163}$. Since 163 is prime, we can use FLT, so

$$314^{162} \equiv 1 \pmod{163}.$$

Problem 8. What is the remainder when 2001^{2001} is divided by 26?

Solution.

This can be rewritten as $2001^{2001} \pmod{26}$. Since 26 is not prime, we can't use FLT, but we can break it into $2001^{2001} \pmod{13}$ and $2001^{2001} \pmod{2}$ and use the remainder theorem as follows,

$$\begin{aligned}
2001^{2001} &\equiv 2001^{1200} \cdot 2001^{801} && \pmod{13} \\
&\equiv \left(2001^{12}\right)^{100} \cdot 2001^{720} \cdot 2001^{81} && \pmod{13} \\
&\equiv 1 \cdot \left(2001^{12}\right)^{60} \cdot 2001^{81} && \pmod{13} \\
&\equiv 1 \cdot 2001^{72} \cdot 2001^{9} && \pmod{13} \\
&\equiv (1300 + 701)^{9} && \pmod{13} \\
&\equiv (0 + 650 + 51)^{9} && \pmod{13} \\
&\equiv (0 + 39 + 12)^{9} && \pmod{13} \\
&\equiv (-1)^{9} && \pmod{13} \\
2001^{2001} &\equiv -1 && \pmod{13}
\end{aligned}$$

Then,

$$\begin{aligned}
2001^{2001} &\equiv (1)^{2001} && \pmod{2} \\
&\equiv 1 && \pmod{2} \\
2001^{2001} &\equiv -1 && \pmod{2}
\end{aligned}$$

Since we have both $2001^{2001} \equiv -1 \pmod{13}$ and $2001^{2001} \equiv -1 \pmod{2}$, since $13 \perp 2$ this means that

$$2001^{2001} \equiv -1 \pmod{26}.$$

3 (Page 55)

Problem 3. Calculate τ and σ of $10115 = 5 \cdot 7 \cdot 17^2$ and $100115 = 5 \cdot 20023$.

Solution.

10115 First we can start with

$$\begin{aligned}
\tau(10115) &= \tau(5) \cdot \tau(7) \cdot \tau(17^2) \\
&= (2) \cdot (2) \cdot (3) \\
\tau(10115) &= 12
\end{aligned}$$

Then,

$$\begin{aligned}
\sigma(10115) &= \sigma(5) \cdot \sigma(7) \cdot \sigma(17^2) \\
&= (5+1) \cdot (7+1) \cdot \left(\frac{17^{2+1} - 1}{17 - 1}\right) \\
&= (48) \cdot \left(\frac{17^3 - 1}{16}\right) \\
&= (3) \cdot (4913 - 1) \\
&= (3) \cdot (4912) \\
\sigma(10115) &= 14736
\end{aligned}$$

100115 For this we start with

$$\begin{aligned}\tau(100115) &= \tau(5) \cdot \tau 20023 \\ &= (2) cdot (2) \\ \tau(100115) &= 4\end{aligned}$$

Then,

$$\begin{aligned}\sigma(100115) &= \sigma(5) \cdot \sigma 20023 \\ &= (5+1) \cdot (20023+1) \\ &= (6) \cdot (20024) \\ \sigma(100115) &= 120144\end{aligned}$$

Problem 5. Show that σn is odd if n is a power of two.

Proof. Let n be a power of two, that is for some positive integer k $n = 2^k$. Then we want to find if $n \pmod 2$ is 0 or 1 to see if σn is even or odd.

$$\begin{aligned}\sigma(n) &= \sigma(2^k) \\ &= \frac{2^{k+1}-1}{2-1} \\ &= 2^{k+1}-1 \\ &\equiv 0-1 \pmod 2 \\ \sigma(n) &\equiv 1 \pmod 2\end{aligned}$$

Since $\sigma(n) \equiv 1 \pmod 2$ we know that $\sigma(n)$ is odd. □

Problem 7. What is the smallest integer n such that $\tau(n) = 8$? Such that $\tau(n) = 10$?

Solution.
Given that $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, we know that $\tau(n) = \prod_{i=1}^{k}(e_i+1)$. Then, if $\tau(n) = 8$ we know that $8 = 2^3$, so we have one of the following: $(e_1+1)(e_2+1)(e_3+1) = (2)(2)(2)$, $(e_1+1)(e_2+1) = (4)(2)$, $(e_1+1)(e_2+1) = (2)(4)$ or $(e_1+1) = 8$. Respectively, with the smallest primes possible (2, 3, and 5) this would be $n = (2)(3)(5) = 30$, $n = (2^3)(3) = 24$, $n = (2)(3^3) = 54$, or $n = (2^7) = 128$. So we can see that for $\tau(n) = 8$ the smallest possible n is 24.

Then for $\tau(n) = 10$, we know that $10 = 2 \cdot 5$, so we have one of the following: $(e_1+1)(e_2+1) = (2)(5)$, $(e_1+1)(e_2+1) = (5)(2)$, or $(e_1+1) = (10)$. Respectively these are $n = (2)(3^4) = 162$, $n = (2^4)(3) = 48$ or $n = 2^9 = 512$. So we can see that for $\tau(n) = 10$, the smallest possible n is 48.

Problem 8. Does $\tau(n) = k$ have a solution for n for each k?

Proof. Given any positive integer k, we know we can find a solution for $\tau(n) = k$ where $n = 2^{k-1}$, no matter what the k, we see that

$$\tau(n) = \tau(2^{k-1}) = (k-1+1) = k$$

So there is always a solution n for each k. □

Problem 9. In 1644, Mersenne asked for a number with 60 divisors. Find one smaller than 10,000.

Solution.

We can see that $60 = 2^2 \cdot 3 \cdot 5$, so based on the past solutions I may guess that the smallest $n's$ will be one of the following: $(e_1+1)(e_2+1)(e_3+1) = (5)(4)(3)$, $(e_1+1)(e_2+1)(e_3+1) = (6)(5)(2)$, or $(e_1+1)(e_2+1)(e_3+1)(e_4+1) = (5)(3)(2)(2)$. Those are respectively $n = (2^4)(3^3)(5^2) = (4)(27)(10^2) = (108)(100) > 10,000$, $n = (2^5)(3^4)(5^1) = (4^2)(3^4)(10) = (16)(81)(10) = (1296)(10) > 10,000$, or $n = (2^4)(3^2)(5^1)(7^1) = (8)(9)(10)(7) = 5040$. So an n smaller than 10,000 with 60 divisors is 5040.

Problem 10. Find infinitely many n such that $\tau(n) = 60$.

Solution.

Using the above calculation, $\tau(n) = 60$ for all n of the form

$$p_a^4 \cdot p_b^3 \cdot p_c^2$$

for any primes p_1, p_2, and p_3. Since there are infinitely many primes, there are then infinitely many $n's$ as well.

Problem 12. For which n is $\sigma(n)$ odd?

Solution.

Let $\sigma(n)$ be odd, then we see

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right)$$

For $\sigma(n)$ to be odd, all of the things in the product have to also be odd, so $\frac{p_i^{e_i+1}-1}{p_i-1}$ must be odd. First we will check for when p_i is even, meaning $p_i = 2$. In this case we have $\frac{2^{e_i+1}-1}{2-1} = 2^{e_i+1} - 1$ which must be odd by definition, so this will always be true.

Then, if p_i is anything other than 2, we can see that for $\frac{p_i^{e_i+1}-1}{p_i-1}$ to be odd, that $\exists k$ where k is odd, s.t.

$$\begin{aligned} p_i^{e_i+1} - 1 &= k(p_i - 1) \\ p_i^{e_i+1} - 1 &= kp_i - k \\ p_i^{e_i+1} - kp_i &= 1 - k \\ p_i(p_i^{e_i} - k) &= 1 - k \end{aligned}$$

Then, take it mod 2, to then see

$$\begin{aligned} 1(1^{e_i} - 1) &\equiv 1 - 1 \mod 2 \\ 1^{e_i} - 1 &\equiv 0 \mod 2 \\ 1^{e_i} &\equiv 1 \mod 2 \\ (-1)^{e_i} &\equiv 1 \mod 2 \end{aligned}$$

This means that we can see that e_i must be even.

So σn is odd only when n has the form,

$$n = 2^{e_1} \cdot p_1^{2e_2} \cdots p_k^{2e_k}.$$

4 (Page 71)

Problem 1. Calculate $\phi(42)$, $\phi(420)$, and $\phi(4200)$.

Solution.

42 Start with $42 = 2 \cdot 3 \cdot 7$, then

$$\begin{aligned}
\phi(42) &= 42\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) \\
&= (42)\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{6}{7}\right) \\
&= (1)(2)(6) \\
\phi(42) &= 12
\end{aligned}$$

420 Start with $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, then

$$\begin{aligned}
\pi 420 &= 420\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) \\
&= (420)\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) \\
&= (2)(1)(2)(4)(6) \\
&= 24 \cdot 4 \\
\phi(420) &= 96
\end{aligned}$$

4200 Start with $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$, then

$$\begin{aligned}
\phi(4200) &= (4200)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) \\
&= (420)\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) \\
&= (20)(1)(2)(4)(6) \\
\phi(4200) &= 960
\end{aligned}$$

Problem 3. Calculate ϕ of $10115 = 5 \cdot 7 \cdot 17^2$ and $100115 = 5 \cdot 20023$.

Solution.

Start with $10115 = 5 \cdot 7 \cdot 17^2$, then

$$\begin{aligned}
\phi(10115) &= (10115)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{17}\right) \\
&= (10115)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\left(\frac{16}{17}\right) \\
&= (17)(4)(6)(16) \\
\phi(10115) &= 6528
\end{aligned}$$

Then, start with $100115 = 5 \cdot 20023$, then

$$\begin{aligned}
\phi(100115) &= (100115)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{20023}\right) \\
&= (100115)\left(\frac{4}{5}\right)\left(\frac{20022}{20023}\right) \\
&= (1)(4)(20022) \\
\phi(100115) &= 80088
\end{aligned}$$

Problem 7. Show that if n is odd, then $\phi(4n) = 2\phi(n)$.

Proof. Let n be odd. Then lets look at $\phi(4n)$,

$$\begin{aligned}
\phi(4n) &= phi(2^2)\phi(n) \\
&= 4\left(1 - \frac{1}{2}\right)\phi(n) \\
&= 4\left(\frac{1}{2}\right)\phi(n) \\
\phi(4n) &= 2\phi(n).
\end{aligned}$$

$\square$

Problem 14. Find four solutions of $\phi(n) = 16$.

Solution.

Let $\phi(n) = 16$, then let $n = p_1^{e_1} \cdots p_k^{e_k}$. For $\phi(n) = 16$ then

$$\begin{aligned}
\phi(n) &= n \prod_{i=1}^{k} \frac{p_i - 1}{p_i} \\
\phi(n) &= n \frac{\prod_{i=1}^{k} p_i - 1}{\prod_{i=1}^{k} p_i} \\
n &= \phi(n) \frac{\prod_{i=1}^{k} p_i}{\prod_{i=1}^{k} p_i - 1} \\
n &= 16 \frac{\prod_{i=1}^{k} p_i}{\prod_{i=1}^{k} p_i - 1} \\
n &= \frac{16}{\prod_{i=1}^{k} p_i - 1} \prod_{i=1}^{k} p_i
\end{aligned}$$

We need to find r_i where $r_i = p_i - 1$, we can see by above that $r_i | 16$, and $r_i + 1$ is prime, so we can list the divisors of 16:

$$r_i = \{1, 2, 4, 8, 16\}$$

Then check for primes in $r_i + 1 = p_i$

$$r_i + 1 = \{2, 3, 5, \cancel{9}, 17\}$$

So our only possibilities for r_i are $\{1, 2, 4, 16\}$ and so we must have p_i in $\{2, 3, 5, 17\}$. Then, going back to our other formula for $\phi(n)$ we can see

$$\begin{aligned}\phi(n) &= p_1^{e_1-1}(p_1-1)\cdot p_2^{e_2-1}(p_2-1)\cdot p_3^{e_3-1}(p_3-1)\cdot p_4^{e_4-1}(p_4-1)\\ 16 &= 2^{e_1-1}(2-1)\cdot 3^{e_2-1}(3-1)\cdot 5^{e_3-1}(5-1)\cdot 17^{e_4-1}(17-1)\end{aligned}$$

We can see that because $16 < 17$, the only cases that 17 can be a factor are 17 and $17\cdot 2$ $(2^0\cdot(1) = 1)$, then look for

$$16 = 2^{e_1-1}(2-1)\cdot 3^{e_2-1}(3-1)\cdot 5^{e_3-1}(5-1)$$

We can see that $5^2 > 16$ so $e_3 < 2$, then we can also see that $3 \nmid 16$, so $e_2 < 2$ as well. Then we have a few possibilities,

$$\begin{array}{lll|ll} 16 = 2^{e_1-1}(2-1)\cdot 2\cdot 4 & \rightarrow e_1 = 2 & & n = & 2^2\cdot 3\cdot 5\\ 16 = 2^{e_1-1}(2-1)\cdot 4 & \rightarrow e_1 = 3 & & n = & 2^3\cdot 5\\ 16 = 2^{e_1-1}(2-1)\cdot 2 & \rightarrow e_1 = 4 & & n = & 2^4\cdot 3\\ 16 = 2^{e_1-1}(2-1) & \rightarrow e_1 = 5 & & n = & 2^5\end{array}$$

So the possibilities for $\phi(n) = 16$ are $n = a$ where a is in $\{2^2\cdot 3\cdot 5, 2^3\cdot 5, 2^4\cdot 3, 2^5, 17, 17\cdot 2\}$

Problem 15. Find all solutions of $\phi(n) = 4$ and prove that there are no more.

Proof. Using the same logic as above, we get to

$$n = \frac{4}{\prod_{i=1}^{k} p_i - 1}\prod_{i=1}^{k} p_i$$

We need to find r_i where $r_i = p_i - 1$, we can see by above that $r_i|4$, and $r_i + 1$ is prime, so we can list the divisors of 4:

$$r_i = \{1, 2, 4\}$$

Then check for primes in $r_i + 1 = p_i$

$$r_i + 1 = \{2, 3, 5\}$$

So our only possibilities for r_i are $\{1, 2, 4\}$ and so we must have p_i in $\{2, 3, 5\}$. Then, going back to our other formula for $\phi(n)$ we can see

$$\begin{aligned}\phi(n) &= p_1^{e_1-1}(p_1-1)\cdot p_2^{e_2-1}(p_2-1)\cdot p_3^{e_3-1}(p_3-1)\cdot p_4^{e_4-1}(p_4-1)\\ 4 &= 2^{e_1-1}(2-1)\cdot 3^{e_2-1}(3-1)\cdot 5^{e_3-1}(5-1)\end{aligned}$$

Since $5 > 4$, we can only have $n = 5$ or $n = 2\cdot 5$. Moving on if 3 is a factor, we are left with

$$4 = 2^{e_1-1}(2-1)\cdot 3^{e_2-1}(2)$$

Since $3^2 > 4$ then $e_2 < 2$, so we can only have

$$\begin{aligned} 4 &= 2^{e_1-1} \cdot 2 \\ 2 &= 2^{e_1-1} \\ e_1 &= 2 \end{aligned}$$

So we get $n = 2^2 \cdot 3$ If 3 is not a factor we have

$$\begin{aligned} 4 &= 2^{e_1-1}(2-1) \\ 4 &= 2^{e_1-1} \\ e_1 &= 3 \end{aligned}$$

Then, $n = 2^3$.

So all the possibilities for n if $\phi(n) = 4$ are $n = a$ where a is in $\{2^3, 2^2 \cdot 3, 2 \cdot 5, 5\}$. □

5

Problem. Compute $\mu(n)$ for $n = 1, 2, ..., 12$.

Solution.

1: $1 = 1^1$

$$\mu(1) = 1$$

2: $2 = 2^1$

$$\begin{aligned} \mu(2) &= (-1)^1 \\ \mu(2) &= -1 \end{aligned}$$

3: $3 = 3^1$

$$\begin{aligned} \mu(3) &= (-1)^1 \\ \mu(3) &= -1 \end{aligned}$$

4: $4 = 2^2$

$$\mu(4) = 0$$

5: $5 = 5^1$

$$\begin{aligned} \mu(5) &= (-1)^1 \\ \mu(5) &= -1 \end{aligned}$$

6: $6 = 2^1 \cdot 3^1$

$$\mu(6) = (-1)^2$$
$$\mu(6) = 1$$

7: $7 = 7^1$

$$\mu(7) = (-1)^1$$
$$\mu(7) = -1$$

8: $8 = 2^3$

$$\mu(8) = 0$$

9: $9 = 3^2$

$$\mu(9) = 0$$

10: $10 = 2^1 \cdot 5^1$

$$\mu(10) = (-1)^2$$
$$\mu(10) = 1$$

11: $11 = 11^1$

$$\mu(11) = (-1)^1$$
$$\mu(11) = 1$$

12: $12 = 2^2 \cdot 3^1$

$$\mu(12) = 0$$

6

Problem. Find all n, $25 < n < 40$ such that $\mu(n) = 1$.

Solution.

All of the n such that $\mu(n) = 1$ are n with an even number of factors that are all unique primes. So any primes are automatically disqualified. Then between 25 and 40, this would include

$$\begin{array}{lll} 26 & = 2 \cdot 13 & \checkmark \\ 27 & = 3^2 \cdots & \times \\ 28 & = 2^2 \cdots & \times \\ 30 & = 2 \cdot 3 \cdot 5 & \times \\ 32 & = 2^2 \cdots & \times \\ 33 & = 3 \cdot 11 & \checkmark \\ 34 & = 2 \cdot 17 & \checkmark \\ 35 & = 5 \cdot 7 & \checkmark \\ 36 & = 3^2 \cdots & \times \\ 38 & = 2 \cdot 19 & \checkmark \\ 39 & = 3 \cdot 13 & \checkmark \end{array}$$

So all n that have $\mu(n) = 1$ between $25 < n < 40$ are $\{26, 33, 34, 35, 38, 39\}$.

7

Problem. Find all non-primes $n < 50$ with $\mu(n) = -1$.

Solution.

Any non-primes $n < 50$ with $\mu(n) = -1$ must have an odd non-zero number of unique primes, it cannot be 5 because the smallest number with 5 unique primes is $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. So it will only be numbers with exactly 3 unique primes, The largest prime it can be must have $2 \cdot 3 \cdot a < 50$ so $a < 8$. Then, there are 4 primes under 8 (2,3,5,7), so there is a total of $\binom{4}{3} = 4$ numbers that this could apply to: $2 \cdot 3 \cdot 5$, $2 \cdot 3 \cdot 7$, $2 \cdot 5 \cdot 7$, $3 \cdot 5 \cdot 7$, which is 30, 42, 70, 105. So there are only two numbers less than 50 that are non-primes with $\mu(n) = -1$ and they are 30 and 42.

8

Problem. Prove that if n is any positive integer, then $\mu(n) \cdot \mu(n+1) \cdot \mu(n+2) \cdot \mu(n+3) = 0$.

Proof. Let n be any positive integer. If we think about $n, n+1, n+2$ and $n+3$, we can see that no matter what, if taken mod 4, one of these will be equivalent to 0 mod 4. Therefore, $\mu(n) \cdot \mu(n+1) \cdot \mu(n+2) \cdot \mu(n+3) = 0$, since at least one of them must be divisible by 4, making it's μ equal to 0, and therefore the product must also be 0. $\square$

9

Problem. A number with k digits, all being 1, is called a *repunit*. For example 11,11111, 111 are all repunits. Show that every odd prime except 5 divides some repunit. (**Hint:** all repunits can always be expressed in the form $\frac{10^k-1}{9}$)

Proof. Assume to the contrary, that $\exists p$ where p is prime an $p \neq 2, 5$, and it does **not** divide any repunit.

When $p \neq 2, 5$ then $p \perp 10$. Then look at one way to represent p not dividing any repunit (let k be any positive integer)

$$\begin{aligned} \tfrac{10^k-1}{9} &\not\equiv 0 \pmod{p} \\ 10^k - 1 &\not\equiv 0 \pmod{p} \\ 10^k &\not\equiv 1 \pmod{p} \end{aligned}$$

But this is not possible since we know that $10^{p-1} \equiv 1 \pmod{p}$ because $10 \perp p$ so p must divide $\frac{10^{p-1}-1}{9}$ which is a repunit. So all odd p except 5 must divide at least one repunit. $\square$

10 Extra Credit

Problem. The notation $a \uparrow\uparrow b$ known as "Knuth's up-arrow notation," denotes the number

$$a^{a^{a^{a^{\cdots^{a^a}}}}}$$

with a tower of $a's$ occurring exactly b times.

Compute the last two digits of $3 \uparrow\uparrow 2000$. That is, the last two digits of

$$3^{3^{3^{3^{\cdots^{3^3}}}}}$$

with a total of 2000 3's occurring in the exponent. (No sage allowed!!)

Solution.

To find the last two digits we want to take this mod 100.

First lets find $\phi(100)$, we know $100 = 2^2 \cdot 5^2$,

$$\begin{aligned}
\phi(100) &= 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) \\
&= 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) \\
&= \frac{100}{2\cdot 5}(1)(4) \\
&= (10)(4) \\
\phi(100) &= 40
\end{aligned}$$

Then, we want to think of how many exponents of 3 to get close to 40, since we know $3^{40} \equiv 1 \pmod{m}$, so lets look on a small scale, thinking of finding the least residue of the exponents mod 40

$$\begin{aligned}
3^{3^3} &\equiv (27)^3 \pmod{40} \\
&\equiv (27)^3 \pmod{40} \\
&\equiv -13^2 \cdot (-13) \pmod{40} \\
&\equiv 169 \cdot (-13) \pmod{40} \\
&\equiv 9 \cdot (-13) \pmod{40} \\
&\equiv 9 \cdot (-3) + 9 \cdot (-10) \pmod{40} \\
&\equiv -27 + -10 + -80 \pmod{40} \\
&\equiv -37 \pmod{40} \\
&\equiv 3 \pmod{40}
\end{aligned}$$

Let's iterate this up to a divisor of 2000,

$$\begin{aligned}
3^{3^{3^{3^3}}} &\equiv (3^3)^{3^{3^3}} \pmod{40} \\
&\equiv (3^3)^3 \pmod{40} \\
&\equiv 3 \pmod{40}
\end{aligned}$$

So again on a small scale, we can see that for some k,

$$\begin{aligned}
(3)^{3^{3^{3^{3^3}}}} &\equiv (3)^{40k+3} \pmod{100} \\
&\equiv 3^{40k} \cdot 3^3 \pmod{100} \\
(3)^{3^{3^{3^{3^3}}}} &\equiv 3^3 \pmod{100}
\end{aligned}$$

This means that we can reduce it iteratively down from $3^{3^{3^{3^{\cdots^{3^3}}}}}$ with 2000 3s (in the exponent) to $3^{3^{3^{3^{\cdots^{3^3}}}}}$ with 1996 3s to $3^{3^{3^{3^{\cdots^{3^3}}}}}$ with 1992 3s to $3^{3^{3^{3^{\cdots^{3^3}}}}}$ with 1988 3s, $\cdots$ to $3^{3^{3^{3^3}}}$ with four 3s, to 3 with zero 3s.

So the last two digits of $3 \upuparrows 2000$ is 03.