Homework 3, Math 4150

1. Exercise Set 2.5, #58. Let a and b be integers not divisible by the prime number p.

   (a) If $a^p \equiv b^p \pmod{p}$, prove that $a \equiv b \pmod{p}$.

   Solution.

   First as a and b are not divisible by p we know that,

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ b^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

   Now multiplying both sides by a and b respective we have,

$$\begin{aligned} a^p &\equiv a \pmod{p} \\ b^p &\equiv b \pmod{p} \end{aligned}$$

   So replacing this in the original congruence we have,

$$\begin{aligned} a \equiv a^p \equiv b^p &\equiv b \pmod{p} \\ a &\equiv b \pmod{p} \end{aligned}$$

   (b) If $a^p \equiv b^p \pmod{p}$, prove that $a^p \equiv b^p \pmod{p^2}$.

   Solution.

   Consider $a^p - b^p$ we can write this as $a^p - b^p = (a-b)S$ where S is the sum. So we have,

$$a^p - b^p \equiv (a-b)S \equiv a - b \pmod{p}$$

   from above. Now rearranging we have,

$$(S-1)(a-b) \equiv 0 \pmod{p}$$

   Now note that $S = a^{p-1} + a^{p-2}b \cdots + ab^{p-2} + b^{p-1} \equiv a^{p-1} + \cdots + a^{p-1} \equiv p \cdot a^{p-1} \equiv 0 \pmod{p}$

   So we have $p \mid S$. Now if $p \mid S$ and $p \mid a - b$ then we have $p^2 \mid S(a-b) = a^p - b^p$. Now, $p^2 \mid a^p - b^p$ which means that $a^p \equiv b^p \pmod{p}^2$.

2. Exercise Set 2.5, #62. The following exercise proves that there are infinitely many odd pseudoprime numbers.

   (a) Let a and b be positive integers such that $a \mid b$. Prove that $2^a - 1 \mid 2^b - 1$.

   Solution.

   If $a \mid b$ then we have $b = ak$. So we need to show $2^a - 1 \mid 2^{ka} - 1$. However we have $(2^a)^k - 1^k = (2^a - 1)(2^{a(k-1)+\cdots})$. So we show that $2^{ka} - 1$ has $2^a - 1$ as a factor which means that $2^a - 1 \mid 2^b - 1$ if $a \mid b$.

   (b) Suppose that n is composite. Prove that n is an odd pseudoprime number if and only if $2^{n-1} \equiv 1 \pmod{n}$.

   Solution.

   ($\Rightarrow$) We are told that n is an odd pseudoprime which means that $2^n \equiv 2 \pmod{n}$ or $22^{n-1} \equiv 2 \pmod{p}$. However as n is odd we know that $2 \nmid n$ or that 2 is co-prime to n which means that 2 has an inverse mod n. Now if we multiply both sides by the inverse of 2 we get $2^{n-1} \equiv 1 \pmod{n}$.

   ($\Leftarrow$) We are given that $2^{n-1} \equiv 1 \pmod{n}$. We know that n is composite hence it's not prime. So n is either even or odd. We see that n can't be even as we have $n \mid 2^{n-1} - 1$ and if n is even we have $2 \mid 2^{n-1} - 1$ and as 2^{n-1} is a power of 2 that means that $2 \mid 1$ which is false. Hence, n is odd. Now we multiply both sides by 2 and we have $2^n \equiv 2 \pmod{n}$ which by definition means that n is a pseudo prime and we showed that it's also prime.

   (c) Prove that if n is an odd pseudoprime number, then $m = 2^n - 1$ is an odd pseudoprime number.

   Solution.

   If n is an odd pseudoprime number then we know that $2^{n-1} \equiv 1 \pmod{n}$ from (b). But this means that $n \mid 2^{n-1} - 1$. However, if $n \mid 2^{n-1} - 1$ then $n \mid 2(2^{n-1} - 1)$. Now using a we get,

   $$2^n - 1 \mid 2^{2^n - 2} - 1$$

   Now take $k = 2^n - 1$ so we have,

   $$k \mid 2^{k-1} - 1$$

   or that

   $$2^{k-1} \equiv 1 \pmod{k}$$

   Which by (b) we have k or that $2^n - 1$ is an odd pseudoprime.

   [**Hint**: Use parts (a) and (b)].

   (d) Prove that there are infinitely many odd pseudoprime numbers.

   Assume there are only finitely many odd pseudoprime numbers, so there exists some maximum odd pseudoprime say n. But from (c) we know that if n is an odd pseuodprime then $2^n - 1$ is also an odd pseuodprime. But we have $2^n - 1 > n$ for $n > 1$ and hence we found an odd pseudoprime $2^n - 1$greater than our maxium n. So our assumption must be wrong that there are only finitely many pseuodprimes and thus there are infinitely many odd pseudoprimes.

3. Exercise Set 2.6 , #68(a),(d) Using Euler's Theorem, find the least nonnegative residue modulo m of each integer n below.

   (a) $n = 29^{198}, m = 20$

   Solution.

   We need $x \equiv 29^{198} \pmod{20}$. First we have $29 \equiv 9 \pmod{20}$ so $x \equiv 9^{198} \pmod{20}$. We have 20 is composite and $20 = 2^2 5$ so $\phi(20) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$. And we have $198 = 8 \cdot 24 + 6$, so, $9^{198} = 9^{8 \cdot 24} 2^6$. But $9^8 \equiv 1 \pmod{20}$ from Euler's theorem (as 9 is coprime to 20), so we have,

   $$x \equiv 9^6 \pmod{20}$$

   Now $9^8 \equiv 1 \pmod{20}$ so multiply both sides by 9^2 we get,

   $$\begin{aligned} 9^2 x \equiv 9^8 \equiv 1 &\pmod{20} \\ 81x \equiv 1 &\pmod{20} \\ 1x \equiv 1 &\pmod{20} \end{aligned}$$

   So $x \equiv 1 \pmod{20}$

   (b) $n = 99^{999999}, m = 26$

   Solution.

   First we have $99 \equiv 21 \pmod{26}$ so we need $x \equiv 21^{999999} \pmod{26}$. Now, $26 = 2 \cdot 13$ so $\phi(26) = 26(1 - \frac{1}{2})(1 - \frac{1}{13}) = 12$. So we have $21^{12} \equiv 1 \pmod{26}$. We have $999999 = 83333 * 12 + 3$ so,

   $$\begin{aligned} x \equiv 21^{999999} \equiv 21^{83333 \cdot 12} 21^3 &\pmod{26} \\ x \equiv 1 \cdot 21^3 &\pmod{26} \end{aligned}$$

   But $21 \equiv -5 \pmod{2}6$ so,

   $$\begin{aligned} x \equiv 21^3 \equiv (-5)^3 &\pmod{26} \\ x \equiv -125 \equiv 5 &\pmod{26} \end{aligned}$$

   So we have $x \equiv 5 \pmod{26}$

4. Exercise Set 2.6, #75. Let m be a positive integer with $m \neq 2$. If $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ is a reduced residue system modulo m, prove that

$$r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0 \pmod{m}.$$

Solution.

For each r_i in the list we know that $(r_i, m) = 1$. Now consider it's negative modulo m that is $m - r_i$ we know that similarly we have $(m - r_i, m) = 1$ as if they did share a common factor then r_i must also share the same factor. Hence $m - r_i$ is also in the same list. As this is true for each r_i and the fact that each of the negative is unique, every element has a negative modulo m in the same list. Hence we have,

$$r_1 + r_2 + \cdots + r_{\phi(m)} \equiv r_1 + r_2 + \cdots + (m - r_2) + (m - r_1) \equiv \frac{1}{2}\phi(m)m \equiv 0 \pmod{m}$$

5. Exercise Set 3.1, #7

Definition: Let $n \in \mathbb{Z}$ with $n > 0$. The Liouville λ-function, denoted $\lambda(n)$, is defined by

$$\lambda(n) := \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \quad \text{where} \quad p_1, \ldots, p_k \\ & \text{are not necessarily distinct prime numbers.} \end{cases}$$

(a) Prove that λ is a completely multiplicative arithmetic function.

Solution.

We need to show that for $m, n \in \mathbb{Z}$ we have $\lambda(mn) = \lambda(m)\lambda(n)$. First, trivially if $m = 1, n = 1$ then $mn = 1$ and we have $f(mn) = f(1) = 1 = 1 \cdot 1 = f(1)f(1) = f(m)f(n)$. So consider the case where $m, n \neq 1$ so let $m = q_1 q_2 \ldots q_k$ where they are not necessarily distinct primes and $n = p_1 p_2 \ldots p_r$ where neither are distinct primes. So we have,

$$\lambda(mn) = \lambda(p_1 p_2 \ldots p_r q_1 q_2 \ldots q_k)$$

In this case the set $p_1 p_2 \ldots p_r q_1 q_2 \ldots q_k$ are primes not necessarily distinct either. So we have $\lambda(mn) = (-1)^{r+k} = (-1)^r(-1)^k = \lambda(m)\lambda(n)$.

(b) Let $F(n) := \sum_{d|n, d>0} \lambda(d)$. Prove that

$$F(n) = \begin{cases} 1 & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise.} \end{cases}$$

Solution. If λ is a multiplicative function that means that $F(n)$ is also a multiplicative function. Hence, it is enough to check how F functions on prime powers. Consider a prime power p^k we have $F(p^k) = \sum_{d|n} \lambda(d) = \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^k) = 1 + (-1) + (-1)^2 + (-1)^3 + \cdots + (-1)^k = 1 + (-1 + 1 - 1 + \cdots + (-1)^k)$.

Now if n is a perfect square then we can write $n = p_1^{a_1} \ldots p_k^{a_k}$ where $a_1, \ldots, a_k$ are even numbers so we have,

$$\begin{aligned} F(n) &= F(p_1^{a_1} \ldots p_k^{a_k}) \\ &= F(p_1^{a_1}) \ldots F(p_k^{a_k}) \end{aligned}$$

Now as $a_1, \ldots, a_k$ are even numbers we have $\lambda(p_i^{a_i}) = 1 + (-1 + 1 + \cdots - 1 + 1) = 1 + 0$ (for every -1 we will have 1 and this is guaranteed as a_i is even). Hence we have

$$F(n) = 1 \cdot \cdots \cdot 1 = 1$$

Now if they are not perfect squares there is some p_i such that it's power is not even i.e. we have p^{a_i} and a_i is odd. So for this prime we have,

$$F(p^{a_i}) = \lambda(1) + \cdots + \lambda(p^{a_i}) = 1 + (-1 + 1 + \ldots (-1)^{a_i}) = 1 + (-1 + 1 \cdots - 1) = 0$$

Hence $F(n) = 0$ as we have at least one zero in the product.

6. Exercise Set 3.2, #12. Let $n \in \mathbb{Z}$ with $n > 1$. If n has prime factorisation $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, prove that

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1).$$

Solution.

We know that $\phi(n)$ is multiplicative so this means that $\phi(p_1^{a_1} \dots p_m^{a_m}) = \phi(p_1^{a_1}) \dots \phi(p_m^{a_m})$ as distinct prime powers are pairwise coprime. Now we know that $\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1}$ as there are $p_i^{a_i-1}$ numbers smaller than $p_i^{a_i}$ that divide $p_i^{a_i}$ as p_i is a prime number. So we have,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1}) \dots \phi(p_m^{a_m}) \\
&= (p_1^{a_1} - p_1^{a_1-1}) \dots (p_m^{a_m} - p_m^{a_m-1}) \\
&= p_1^{a_1-1}(p_1 - 1) \dots p_m^{a_m-1}(p_m - 1) \\
&= p_1^{a_1-1} \dots p_m^{a_m-1}(p_1 - 1) \dots (p_m - 1) \\
&= p_1^{a_1-1} \dots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1)
\end{aligned}$$

7. Exercise Set 3.2, #15. Let $k \in \mathbb{Z}$ with $k > 0$. Prove that the equation $\phi(n) = k$ has at most finitely many solutions. [Hint: Use Question 6]

Solution.

We know from question 6 that for a given n we have

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1)$$

. So for a fixed k the solution n would be of the form $n = p_1^{a_1} \dots p_m^{a_m}$ such that,

$$p_1^{a_1-1} p_2^{a_2-1} \cdots p_m^{a_m-1} \prod_{i=1}^{m} (p_i - 1) = k$$

Now for each prime in the above we have $(p_i - 1) \mid k$ which means that p_i is at most $k + 1$ as if it was bigger than that then $p_i - 1$ would be larger than k and hence won't be able to divide k. So any prime in the list is $p_i \le k + 1$. Note that there are only a finite number of primes smaller equal $k + 1$. Now consider $p_i^{a_i-1}$ we know that this divides k. Similar to the above argument a_i is also bounded as for some $p_i^{a_i-1}$ increases as a_i increases and at some point it is greater than k and hence can't divide k. So this means that each a_i is bounded above as well. So we've shown that there are only a finite number of p_i and a_i which means that there is only a finite number of n such that $\phi(n) = k$

8. Exercise Set 3.2, #16. Let n be a positive integer.

   (a) Prove that $\sqrt{n}/2 \leq \phi(n) \leq n$.

   Solution.

   First we show the upperbound. We know $\phi(n)$ counts the number of numbers coprime to n smaller than n so by definition as we're counting numbers smaller than n there is only a maximum of n choices. More formally we have $\phi(n) = n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_2})$. And we have $(1-\frac{1}{p_i}) < 1$ which means that $\prod_i(1-\frac{1}{p_i}) < 1$ so $n\prod_i(1-\frac{1}{p_i}) = \phi(n) < n$.

   For the lower bound we can make the following simplifications,

$$\begin{aligned}\frac{\sqrt{n}}{2} &\leq \phi(n)\\ \frac{\sqrt{n}}{2} &\leq n\prod_i\left(1-\frac{1}{p_i}\right)\\ \frac{1}{2} &\leq \sqrt{n}\prod_i\left(1-\frac{1}{p_i}\right)\end{aligned}$$

   Now we know that $n = p_1^{a_1}\dots p_n^{a_n}$. So $n \geq p_1\dots p_n$ and $\sqrt{n} \geq \sqrt{p_1\dots p_n}$. So it is enough to show that,

$$\frac{1}{2} \leq \sqrt{p_1\dots p_n}\prod_i\left(1-\frac{1}{p_i}\right)$$

   Now for $p = 2$ and for one prime we have $\sqrt{2}/2 = 1/\sqrt{2} \geq 1/2$. For every subsequence prime addition we have $\sqrt{p}(p-1)/p = (p-1)/\sqrt{p}$. But for $p > 2$ $p-1 \geq \sqrt{p}$ which means that the entire multiplication by $\sqrt{p}\left(1-\frac{1}{p}\right)$ is greater than 1 and hence will not decrease the product in the RHS. Hence the minimum value of the RHS is when we have only $p = 2$ where we get $\frac{1}{\sqrt{2}}$ and hence,

$$\frac{1}{2} \leq \sqrt{p_1\dots p_n}\prod_i\left(1-\frac{1}{p_i}\right)$$

   and this is equivalent to stating that $\phi(n) \geq \sqrt{n}/2$

   (b) If n is composite, prove that $\phi(n) \leq n - \sqrt{n}$.

   [Hint: Use Question 1 for part (a) and Theorem 3.4 for part (b)]

   Solution.

We can make the following simplifications,

$$\begin{aligned}
\phi(n) &\leq n - \sqrt{n} \\
n \prod_i \left(1 - \frac{1}{p_i}\right) &\leq n\left(1 - \sqrt{n}/n\right) \\
n \prod_i \left(1 - \frac{1}{p_i}\right) &\leq n\left(1 - \frac{1}{\sqrt{n}}\right) \\
\prod_i \left(1 - \frac{1}{p_i}\right) &\leq \left(1 - \frac{1}{\sqrt{n}}\right)
\end{aligned}$$

So it is enough to show that $\prod_i \left(1 - \frac{1}{p_i}\right) \leq \left(1 - \frac{1}{\sqrt{n}}\right)$. Now as $n = p_1^{a_1} \ldots p_n^{a_n}$ we have $n \geq p_1 \ldots p_n = \prod p_i = x$. So we have $\sqrt{n} \geq \sqrt{x}$ or that $\frac{1}{\sqrt{x}} \geq \frac{1}{\sqrt{n}}$ or $1 - \frac{1}{\sqrt{x}} \leq 1 - \frac{1}{\sqrt{n}}$. So it is enough to show that,

$$\prod_i \left(1 - \frac{1}{p_i}\right) \leq \left(1 - \frac{1}{\sqrt{p_1 \cdots p_n}}\right)$$

We can show this by induction, consider for base case p_1, p_2 we have,

$$\begin{aligned}
\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) &= 1 - \frac{1}{p_2} - \frac{1}{p_1} + \frac{1}{p_1 p_2} \\
&= 1 - \frac{(p_1 + p_2) - 1}{p_1 p_2}
\end{aligned}$$

So we need to show,

$$\begin{aligned}
\frac{p_1 + p_2 - 1}{p_1 p_2} &\geq \frac{1}{\sqrt{p_1 p_2}} \\
p_1 + p_2 - 1 &\geq \sqrt{p_1 p_2} \\
p_1^2 + p_2^2 + 1 - 2p_1 - 2p_2 + p_1 p_2 &\geq p_1 p_2 \\
p_1^2 + p_2^2 + 1 - 2p_1 - 2p_2 &\geq 0
\end{aligned}$$

Here for $p > 2$ we always have $p^2 \geq 2p$ so the above is true and hence the base case is true.

Now assume true for primes $p_1, \ldots, p_k$ so we have,

$$\prod_i^k \left(1 - \frac{1}{p_i}\right) \leq 1 - \frac{1}{\sqrt{p_1 \cdots p_k}}$$

Now consider p the $k+1'th$ prime. So we have,

$$\prod_{i}^{k+1}\left(1-\frac{1}{p_i}\right) \leq \left(1-\frac{1}{\sqrt{p_1 \dots p_k}}\right)\left(1-\frac{1}{p}\right)$$

Now using the base case we have,

$$\left(1-\frac{1}{\sqrt{p_1 \dots p_k}}\right)\left(1-\frac{1}{p}\right) \leq \left(1-\frac{1}{\sqrt{p\sqrt{p_1 \dots p_k}}}\right)$$

But we know that $p_1 \dots p_k \geq \sqrt{p_1 \dots p_k}$ so,

$$\begin{aligned} p_1 \dots p_k &\geq \sqrt{p_1 \dots p_k} \\ pp_1 \dots p_k &\geq p\sqrt{p_1 \dots p_k} \\ 1/\sqrt{pp_1 \dots p_k} &\leq 1/\sqrt{p\sqrt{p_1 \dots p_k}} \\ 1 - 1/\sqrt{pp_1 \dots p_k} &\geq 1 - 1/\sqrt{p\sqrt{p_1 \dots p_k}} \end{aligned}$$

So we get,

$$\left(1-\frac{1}{\sqrt{p_1 \dots p_k}}\right)\left(1-\frac{1}{p}\right) \leq \left(1-\frac{1}{\sqrt{p\sqrt{p_1 \dots p_k}}}\right) \leq 1-\frac{1}{pp_1 \dots p_k}$$

or that,

$$\prod_{i}^{k+1}\left(1-\frac{1}{p_i}\right) \leq 1-\frac{1}{\sqrt{p_1 \dots p_{k+1}}}$$

which completes the induction step. Hence proving the statement.