Homework 5

Sean Eva

April 2022

1. *Proof.*

$$\begin{aligned}
10!+1 &= 10*9*8*7*6*5*4*3*2*1+1(\mod 11)\\
10!+1 &= (4*3)(2*6)(8*7)(9*5)*10+1(\mod 11)\\
10!+1 &= (12)(12)(56)(45)*10+1(\mod 11)\\
10!+1 &= (1)(1)(1)(1)*10+1(\mod 11)\\
10!+1 &= 11(\mod 11)\\
10!+1 &= 0(\mod 11).
\end{aligned}$$

□

17. *Proof.* It will be useful to employ Wilson's Theorem, which states that if p is a prime, then, $(p-1)! \equiv -1(\mod p)$. Also that $(p-1)! = (p-1)(p-2)(p-3)!$ allows for $(p-1)! \equiv (-2)(-1)(p-3)!(\mod p)$ which further implies that $2(p-3)! \equiv -1(\mod p)$. □

41. *Proof.* Given p is a prime, then $1*2*...*(p-1) \equiv (p+1)(p+2)...(2p-1)(\mod p)$ each factor is prime to p. So $1 \equiv \frac{(p+1)(p+2)...(2p-1)}{1*2*...*(p-1)}(\mod p)$. Therefore, $2 \equiv \frac{(p+1)(p+2)...(2p-1)(2p)}{1*2*...*(p-1)}(\mod p)$ which means that $\binom{2p}{p}(\mod p)$ □

45. (a) If $c < 26$ then c cards are put into the deck above the card so it ends up in the $2c$ position and $2c < 52$. So $b = 2c$, if $c \geq 26$ then the card is in the $c-26th$ place in the bottom half of the deck. In teh shuffle $c-26-1$ cards are put into the deck above the card so it ends up in the $b = (c-26+c-26-1)th$ place then $b = 2c-53 \equiv 2c(\mod 53)$.

    (b) Since the shuffling is occuring in such a way that card at each shuffle chooses a different position and does not repeat the position until it goes over all the possible 51 positions and hence the required shuffle of number is $51+1 = 52$.

1. *Proof.* For 91 to be pseudoprime base 3 would mean that it can be defined as q and write $3^q \equiv 3(\mod q)$ which is true as $3^91 \equiv 3(\mod 91)$. However, we know that $91 = 7*13$ which means that it is composite. Therefore we know that 91 is pseudoprime base 3. □

9. *Proof.* Since we know that n is a pseudoprime to the bases a and b then we know that $a^n \equiv a(\mod n)$ and $b^n \equiv b(\mod n)$. So then we get,

$$\begin{aligned}
a^n*b^n &= a*a*a*a*...*a*b*b*b*b*...*b\\
a^nb^n &= (ab)^n\\
a^nb^n &= a*b(\mod n)\\
(ab)^n &= ab(\mod n).
\end{aligned}$$

Therefore given that n is pseudoprime to bases a and b we know then that n is pseudoprime to base ab. □

3. *Proof.* Let $m > 2$ then $\phi(m)$ is even number. Also if $gcd(a, m) = 1$ if and only if $gcd(m-1, m) = 1$. So we arrange $c_1, c_2, ..., c_{\phi(m)}$ such that $c_{\phi(m)} = m-c_1, c_{\phi(m)-1} = m-c_2$. So $c_1, c_2, ..., c_{\phi(m)/2}, (m-c_1), (m-c_2), ..., m-c_{\phi(m)/2}$ is the complete list of reduced residue system. So $c_1+c_2+...+c_{\phi(m)} = \frac{\phi(m)}{2} * m \equiv 0(\mod m)$. Thus $c_1 + c_2 + ... + c_{\phi(m)} \equiv 0(\mod m)$ □

6. *Proof.* It will be important to notice that $\phi(10) = 4$ and that implies that $7^4 \equiv 1(\mod 10)$. Then we get,

$$\begin{aligned} 7^{999999} &\equiv 7^3 * 1(\mod 10) \\ &\equiv 343(\mod 10) \\ &\equiv 3(\mod 10). \end{aligned}$$

□

14. *Proof.* Consider $M_k = M/m_k = m_1 m_2 ... m_{k-1} m_{k+1} ... m_r$ for the above congruency, if $j \neq k$ then $(M_j, m_k) = 1$. Therefore, $(M_k, m_k) = 1$. Now M_k has an inverse m_k we will denote y_k which means that $M_k y_k \equiv 1(\mod m_k)$. Therefore, the sum can be written as $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r$. The integer x is a simultaneous solution of the r congruences. And because $m_k | M_j$ whenever $j \neq k$, therefore, $M_j \equiv 0(\mod m_k)$. Thus, in the sum of x, all terms except the kth term are congruent to $0(\mod m_k)$. And because $M_k y_k \equiv 1(\mod m_k)$. Put the values in the equation to get $x \equiv a_1 M_1^{\phi(m_1)} + ... + a_r M_r^{\phi(m_r)}(\mod M)$ as desired. □

5. *Proof.* Given that $\phi(n)$ is multiplicative. Let $n = 2^a p_1^b p_2^c ... p_k^\alpha$ where p_i are distinct odd primesm the $b, c, ..., \alpha \geq 1$ and $a \geq 0$. Then, $\phi(n) = \phi(2^a)\phi(p_1^b)...\phi(p_k^\alpha)$. We find all n such that $\phi(n) = 6$. If $k \geq 2$, then since $\phi(p_i^{e_i})$ is even, $\phi(n)$ is divisible by 4, so cannot be equal to 6. If $k = 0$ we cannot have $\phi(n) = 6$. We conclude that $k = 1$. Thus n must have the shape $2^a p^e$, where $a \geq 0$ and p is an odd prime. But $\phi(p^e) = p^{e-1}(p-1)$. It follows that $p \leq 7$. If $p = 7$, then $p - 1 = 6$, so we must have $e = 1$ and $\phi(2^a) = 1$. This gives the solutions $n = 7$ and 14. We cannot have $p = 5$ because $4 | \phi(5^e)$. Let $p = 3$. If $e \geq 3$, then $\phi(e^e) \geq (3^2)(2)$. So we are left with the possibilities that $e = 1, 2$. If $e = 1$, then $\phi(n) = \phi(2^a)(2)$. This is cannot be 6. Finally if $e = 2$, then $\phi(3^2) = 6$. So to have that $\phi(2^a 3^2) = 6$, we need $\phi(2^a) = 1$ which gives us that $n = 9, 18$. Therefore, all the solutions to $\phi(n) = 6$ are $n = 7, 9, 18$. □

11. *Proof.* Consider that 3 does not divide n. Then $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$ which implies that $\phi(3n) \neq 3\phi(n)$. Alternatively, consider that $3|n$ then let $n = 3^k * m$ where m is not divisible by 3, and $k \geq 1$. Then $\phi(n) = \phi(3^k m) = 2 * 3^{k-1}\phi(m)$; also, $3n = 3^{k+1}m$, so $\phi(3n) = 2 * 3^k \phi(m) = 3\phi(n)$. Therefore, the only numbers that the statement $3\phi(n) = \phi(3n)$ is true is for n that are divisible by 3. □

36. *Proof.* Consider positive integers m and n. Soncider the function f such that $f(n) = \frac{\phi(n)}{n}$ and $f(m) = \frac{\phi(m)}{m}$. Therefore, we get that $f(mn) = \frac{\phi(mn)}{mn}$ or, $f(mn) = \frac{mn\Pi(1-\frac{1}{p_i})\Pi(1-\frac{1}{q_i})}{mn} = \frac{m\Pi(1-\frac{1}{p_i})}{m}\frac{n\Pi(1-\frac{1}{q_i}}{n} = \frac{\phi(m)}{m}\frac{\phi(n)}{n} = f(m)f(n)$. Therefore, the considered function is completely multiplicative. □

4. *Proof.* We will show first that $\sigma(n)$ is odd if n is a power of 2. Suppose that $n = 2^\alpha$, then $\sigma(2^\alpha) = \sum_{d|2^\alpha} d = 1 + 2 + 2^2 + ... + 2^\alpha = \frac{2^{\alpha+1}-1}{2-1} = 2^{\alpha+1} - 1$, and $\sigma(2^\alpha) = 2^{\alpha+1} - 1$ is odd for all integers $\alpha \geq 0$. Next suppose that p is an off prime and that α is a positive integer, then $\sigma(p^\alpha) = 1 + p + p^2 + ... + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$, and $\sigma(p^\alpha)$ is odd if and only if the sum contains an odd number of terms, that is, if and only if α is an even integer. From the fundamental theorem of arithmetic, we see that $\sigma(n)$ is odd if and only if in the prime power decomposition of n every odd prime occurs to an even power, that is, if and only if n is a perfect square or n is 2 times a perfect square. □