Math 209-16 Homework 3

Due Date: 5pm, Oct 13, 2022

P1.(1 pt) Solve the congruence $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.

SOLUTION. The congruence $x^3-9x^2+23x-15 = (x-1)(x-3)(x-5) \equiv 0 \pmod{143}$ is equivalent to $11 \mid (x-1)(x-3)(x-5)$ and $13 \mid (x-1)(x-3)(x-5)$, i.e.,

$$x \equiv 1 \text{ or } 3 \text{ or } 5 \pmod{11} \qquad \text{and} \qquad x \equiv 1 \text{ or } 3 \text{ or } 5 \pmod{13}.$$

By the Chinese Remainder Theorem, $x \equiv a \pmod{11}$ and $x \equiv b \pmod{13}$ is equivalent to $x \equiv 11 \cdot 6 \cdot b + 13 \cdot 6 \cdot a = 66b + 78a \pmod{143}$ since $11 \cdot 6 \equiv 1 \pmod{13}$ and $13 \cdot 6 \equiv 1 \pmod{11}$. Plug in $a, b \in \{1, 3, 5\}$ in the above formula, we get all the solutions $x \equiv 1, 133, 122, 14, 3, 135, 27, 16, 5 \pmod{143}$.

P2.(2 pts) Find all positive integers n such that $\phi(n) \mid n$.

SOLUTION. $n = 1$ trivially satisfies the condition, we next assume $n > 1$ and write $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, where $p_1 < \cdots < p_k$ are prime numbers and $t_1, \ldots, t_k, k$ are positive integers. Now $\phi(n) \mid n$ means

$$[p_1^{t_1-1} \cdots p_k^{t_k-1}(p_1 - 1) \cdots (p_k - 1)] \,\Big|\, p_1^{t_1} \cdots p_k^{t_k},$$

i.e., $(p_1 - 1) \cdots (p_k - 1) \mid p_1 \cdots p_k$. For this to hold, first note that p_1 must be 2, because any prime divisor of $p_1 - 1$ would be less than all the p_i's and hence cannot divide the right hand side, and so $p_1 - 1 = 1$. If $k = 1$, we obtain $n = 2^t$, where t is a positive integer. If $k > 1$, then $p_2, \ldots, p_k$ are odd primes, and so $2 \parallel p_1 \ldots p_k$. Then it follows that k must be 2 since $p_2 - 1, \cdots, p_k - 1$ are all even numbers, and there cannot be more than one of them. Thus we are looking for odd primes p such that $(p-1) \mid 2p$. As the only positive divisors of $2p$ are $1, 2, p, 2p$, this happens only when $p - 1 = 2$, i.e., $p = 3$. In conclusion, all the positive integers n such that $\phi(n) \mid n$ are 2^t for $t \geqslant 0$, and $2^{t_1} 3^{t_2}$ for $t_1, t_2 > 0$.

P3.(2 pts) Let $\psi(n)$ denote the number of integers a, $1 \leqslant a \leqslant n$, for which both $(a,n) = 1$ and $(a+1,n) = 1$. Show that $\psi(n) = n\prod_{p|n}(1-2/p)$. For what values of n is $\psi(n) = 0$?

Proof. When $n = 1$, by definition we have $\psi(n) = 1$. Now we assume that $n > 1$. Let $n = p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$ be the prime factorization of n. Notice that

$$(a,n) = (a+1,n) = 1 \iff a \not\equiv 0, -1 \pmod{p_i},\ \forall\, i \in \{1,\ldots,k\}$$

which means that the number of possible choices for $a \pmod{p_i^{t_i}}$ is $p_i^{t_i-1}(p_i-2)$ for each i. These, together with the Chinese Remainder Theorem, shows the number of possible choices for $a \pmod{n}$ is given by

$$\psi(n) = \prod_i [p_i^{t_i-1}(p_i-2)] = n\prod_{p|n}(1-\frac{2}{p})$$

Moreover, $\psi(n) = 0$ if and only if some p_i equals 2, in other words, $\psi(n) = 0$ exactly for all the even numbers n. $\square$

P4.(2 pts) Let k be a positive integer such that $6k+1 = p_1$, $12k+1 = p_2$, and $18k+1 = p_3$ are all prime numbers, and put $m = p_1p_2p_3$. Show that $(p_i - 1) \mid (m-1)$ for $i = 1, 2, 3$. Deduce that if $(a, p_i) = 1$, then $a^{m-1} \equiv 1 \pmod{p_i}$, $i = 1, 2, 3$. Conclude that if $(a,m) = 1$ then $a^{m-1} \equiv 1 \pmod{m}$, that is, that m is a Carmichael number.

Proof. We compute directly that $m - 1 = (6k+1)(12k+1)(18k+1) - 1 = 6 \cdot 12 \cdot 18k^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)k^2 + (6 + 12 + 18)k$, which is easily seen to be a multiple of $p_i - 1 = 6ik$ for $i = 1, 2, 3$. As a consequence, if $(a, p_i) = 1$ then $a^{m-1} \equiv 1 \pmod{p_i}$ since $a^{p_i-1} \equiv 1 \pmod{p_i}$ by Fermat's little theorem. Since $(a, p_i) = 1$ for all i if and only if $(a,m) = 1$, and $a^{m-1} \equiv 1 \pmod{p_i}$ for all i if and only if $a^{m-1} \equiv 1 \pmod{m}$ by the Chinese Remainder Theorem, it follows that m is a Carmichael number. $\square$

P5.(2 pts) Write $1/1+1/2+\cdots+1/(p-1) = a/b$ with $(a,b) = 1$. Show that $p^2 \mid a$ if $p \geqslant 5$.

Proof. Since $(p-1)! \cdot \frac{a}{b} = \sigma_{p-2} \equiv 0 \pmod{p^2}$ by Wolstenholme's congruence, it follows immediately that $p^2|a$. $\square$

P6.(2 pts) Show that if $p \geqslant 5$ is a prime and m is a positive integer then $\binom{mp-1}{p-1} \equiv 1 \pmod{p^3}$.

Proof. Since $\binom{mp-1}{p-1} = \frac{(mp-1)\cdots(mp-p+1)}{(p-1)!}$ and $((p-1)!, p) = 1$, we only need to prove that $(mp-1)(mp-2)\cdots(mp-p+1) - (p-1)! \equiv 0 \pmod{p^3}$. Since we have

$$(mp-1)\cdots(mp-p+1)-(p-1)! = (mp)^{p-1} - \sigma_1 (mp)^{p-2} + \cdots + \sigma_{p-3}(mp)^2 - \sigma_{p-2}(mp),$$

so it is indeed divisible by p^3 since $p \mid \sigma_i$ for all i and $p^2 \mid \sigma_{p-2}$. $\square$

P7.(3 pts) Suppose that p is an odd prime, and write $1/1-1/2+1/3-\cdots-1/(p-1) = a/(p-1)!$. Show that $a \equiv (2-2^p)/p \pmod{p}$.

Proof. Using binomial expansion we have:

$$\frac{2-2^p}{p} = -\frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i} = -\sum_{i=1}^{p-1}\frac{(p-1)!}{i!(p-i)!} = -\sum_{i=1}^{p-1}\frac{(p-1)\cdots(p-i+1)}{i!},$$

For any $i \in \{1, 2, \ldots, p-1\}$, let i^{-1} denote its inverse $\pmod{p}$ in $(\mathbb{Z}/p\mathbb{Z})^*$. Then we have the following:

$$\frac{(p-1)\cdots(p-i+1)}{i!} - (-1)^{i-1}i^{-1} = \frac{(p-1)\cdots(p-i+1) - (-1)^{i-1}i!i^{-1}}{i!},$$

but $(p-1)\cdots(p-i+1) - (-1)^{i-1}i!i^{-1} \equiv (-1)\cdots(-i+1) - (-1)^{i-1}(i-1)! \equiv 0 \pmod{p}$, and $(i!, p) = 1$, it follows that

$$\frac{(p-1)\cdots(p-i+1)}{i!} \equiv (-1)^{i-1}i^{-1} \pmod{p}.$$

Therefore, $\frac{2-2^p}{p} \equiv \sum_{i=1}^{p-1}(-1)^i i^{-1} \pmod{p}$. On the other hand, $\frac{(p-1)!}{i} \equiv -i^{-1} \pmod{p}$ for any $i \in \{1, 2, \cdots, p-1\}$ since $(p-1)! \equiv -1 \pmod{p}$ by Wilson's theorem. As a result, we get

$$a = \sum_{i=1}^{p-1}(-1)^{i-1}\frac{(p-1)!}{i} \equiv \sum_{i=1}^{p-1}(-1)^i i^{-1} \equiv \frac{2-2^p}{p} \pmod{p}$$

The proof is now completed. $\square$

P8.(2 pts) Show that if a^k+1 is prime and $a>1$ then k is a power of 2. Show that if $p \mid (a^{2^n}+1)$ then $p=2$ or $p \equiv 1 \pmod{2^{n+1}}$.

PROOF. If there is an odd prime q dividing k, write $k=qt$, then we have

$$a^k+1 = a^{qt}+1 = (a^t+1)\sum_{i=0}^{q-1}(-a^t)^i$$

which is divisible by a^t+1. But $1 < a^t+1 < a^k+1$, this would contradict the assumption that a^k+1 is a prime. Thus k must be a power of 2.

Now assume p is an odd prime dividing $a^{2^n}+1$. We have $a^{2^n} \equiv -1 \pmod{p}$, and hence $a^{2^{n+1}} \equiv 1 \pmod{p}$. Moreover, 2^{n+1} must be the order of $a \pmod{p}$, otherwise, its order would be a divisor of 2^n and would lead to $a^{2^n} \equiv 1 \pmod{p}$, which is not the case. Therefore 2^{n+1}, as the order of $a \pmod{p}$, must divide $p-1$, since $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. In other words, $p \equiv 1 \pmod{2^{n+1}}$. $\square$

P9.(2 pts) Prove that if a belongs to the exponent 3 modulo a prime p, then $1+a+a^2 \equiv 0 \pmod{p}$, and $1+a$ belongs to the exponent 6.

PROOF. By assumption we have $a^3 \equiv 1 \pmod{p}$, hence $p \mid (a-1)(1+a+a^2)$. But $a \not\equiv 1 \pmod{p}$, so $1+a+a^2 \equiv 0 \pmod{p}$. It follows that $(1+a)^6 = (1+2a+a^2)^3 \equiv a^3 \equiv 1 \pmod{p}$. But $(1+a)^2 \equiv a \not\equiv 1 \pmod{p}$, and $(1+a)^3 = 1+3a(a+1)+a^3 \equiv 1-3+1 = -1 \not\equiv 1 \pmod{p}$, so we conclude that 6 is the order of $1+a \pmod{p}$. $\square$

P10.(2 pts) Show that the number of reduced residues $a \pmod{m}$ such that $a^{m-1} \equiv 1 \pmod{m}$ is exactly $\prod_{p|m}(p-1, m-1)$.

PROOF. Let $m = p_1^{k_1} \cdots p_t^{k_t}$ be the prime factorization of m. By the Chinese Remainder Theorem, $a^{m-1} \equiv 1 \pmod{m}$ is equivalent to $a^{m-1} \equiv 1 \pmod{p_i^{k_i}}$, $\forall\, i$. Suppose $p_i \geqslant 3$ or $p_i = 2$ and $k_i = 1$ or 2, then we see that $a^{m-1} \equiv 1 \pmod{p_i^{k_i}}$ has $n_i = (\phi(p_i^{k_i}), m-1)$ solutions by considering $a = r^n$, where r is the primitive root modulo $p_i^{k_i}$. But $n_i = (\phi(p_i^{k_i}), m-1) = (p_i^{k_i-1}(p_i-1), m-1) = (p_i-1, m-1)$ since $p_i \mid m$, and hence $p_i \nmid (m-1)$. It remains to check the case that $p_i = 2$ and $k_i \geqslant 3$. Since $2 \mid m$, we have $m-1$ is odd. Therefore, $a^{m-1} \equiv 1 \pmod{2^{k_i}}$ has exactly $1 = (2-1, m-1)$ solution. In summary, the number of reduced residues $a \pmod{m}$ such that $a^{m-1} \equiv 1 \pmod{m}$ is $\prod_{p|m}(p-1, m-1)$. $\square$