Problemset 4

Albert Ye

September 23, 2022

1 Modular Practice

a) $9x + 5 \equiv 7 \pmod{11} \implies 9x \equiv 2 \pmod{11} \implies x \equiv 2 \cdot 9^{-1} \pmod{11} \implies x \equiv 2 \cdot 5 \equiv \boxed{10} \pmod{11}$.

b) $3x + 15 \equiv 4 \pmod{21} \implies 3x \equiv -11 \pmod{21}$. However, as $\gcd(3, 21) = 3$, we will need $3x \equiv k \pmod{21}$ where $k \equiv 0 \pmod{3}$. Therefore, there are no solutions to $3x \equiv -11 \pmod{21}$.

c)

$$\begin{aligned} 3x + 2y &\equiv 0 \pmod{7} \\ 2x + y &\equiv 4 \pmod{7} \\ \implies 4x + 2y &\equiv 1 \pmod{7} \\ \implies x &\equiv 1 \pmod{7}. \end{aligned}$$

Substituting for x,

$$\begin{aligned} 2 + y &\equiv 4 \pmod{7} \\ \implies y &\equiv 2 \pmod{7}. \end{aligned}$$

$$\implies \boxed{x \equiv 1 \pmod{7}}, \boxed{y \equiv 2 \pmod{7}}.$$

d) $13^{2019} \equiv x \pmod{12} \implies 1^{2019} \equiv x \pmod{12} \implies \boxed{x \equiv 1 \pmod{12}}$.

e) $7^{10} \equiv 1 \pmod{11}$ from Fermat's Little Theorem, so $7^{21} \equiv 7 \cdot 7^{20} \equiv \boxed{7 \pmod{11}}$.

2 Nontrivial Modular Solutions

a) Because $7^3 \equiv 0 \pmod 7$, we have $(7a+k)^3 \equiv (7a)^3 + (7a)^2k + (7a)k^2 + k^3 \equiv k^3 \pmod 7$. Thus, if $j \equiv k \pmod 7$, then $j^3 \equiv k^3 \pmod 7$. It follows to check the first 7 perfect cubes modulo 7. Those would be $0^3 \equiv 0 \pmod 7, 1^3 \equiv 1 \pmod 7, 2^3 \equiv 1 \pmod 7, 3^3 \equiv 6 \pmod 7, 4^3 \equiv 1 \pmod 7, 5^3 \equiv 6 \pmod 7$, and $6^3 \equiv 6 \pmod 7$. Therefore, the only three possible perfect cubes modulo 7 are $\boxed{0, 1, 6}$.

b) $a^3 + 2b^3 \pmod 7$ can have a few possibilities.

Clearly, we can have $a \equiv b \equiv 0 \pmod 7$, which will give $a^3 + 2b^3 \equiv 0 \pmod 7$. Now, we claim that this is the only way to get 0 (mod 7). Clearly if $a^3 \equiv 0 \pmod 7$ and $b^3 \not\equiv 0 \pmod 7$ then $a^3 + 2b^3 \not\equiv 0 \pmod 7$, and similarly for $b^3 \equiv 0 \pmod 7$ and $a^3 \not\equiv 0 \pmod 7$. The easiest way to prove this claim for cases where both $a^3 \not\equiv 0$ and $b^3 \not\equiv 0$ would be to loop over all possibilities of (a, b) and verify that none satisfy the condition. From part (a), we can group those into cases where a^3 and b^3 equal either 1 or 6.

Case 1: $a^3 \equiv 1 \pmod 7, b^3 \equiv 1 \pmod 7$. Then $a^3 + 2b^3 \equiv 1 + 2 \equiv 3 \pmod 7$.

Case 2: $a^3 \equiv 1 \pmod 7, b^3 \equiv 6 \pmod 7$. Then $a^3 + 2b^3 \equiv 1 + 12 \equiv 13 \equiv -1 \pmod 7$.

Case 3: $a^3 \equiv 6 \pmod 7, b^3 \equiv 1 \pmod 7$. Then $a^3 + 2b^3 \equiv 6 + 2 \equiv 8 \equiv 1 \pmod 7$.

Case 4: $a^3 \equiv 6 \pmod 7, b^3 \equiv 6 \pmod 7$. Then $a^3 + 2b^3 \equiv 6 + 12 \equiv 18 \equiv 4 \pmod 7$.

c) From part (b), we have that $a^3 + 2b^3$ only divides 7 when $a \equiv b \equiv 0 \pmod 7$. Therefore, we would need $a \equiv b \equiv 0 pmod 7$ in order for $a^3 + 2b^3 = 7a^2b$ to hold. Let $a = 7p$ and $b = 7q$. Then, our equation becomes $(7p)^3 + 2(7q)^3 = 7(7p)^2(7q) \implies 343(p^3 + 2q^3) = 2401p^2q \implies p^3 + 2q^3 = 7p^2q$. This means that 7 must also divide (p, q).

Therefore, in order for (a, b) to satisfy this relation, we will need $7^k | a, b$ for all $k \in \mathbb{Z}^*$. The only values of a and b that can satisfy this condition would be $a = 0, b = 0$, so there are no nontrivial solutions for (a, b). $\square$

3 Wilson's Theorem

For the if direction, we know that $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$. Now, we examine all of these indices modulo p. Because p is prime, we know that every residue from 1 to $p-1$ has an inverse modulo p. However, we also know that 1's inverse is 1, and $p-1$'s inverse is $p-1$ because $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \pmod{p}$. Therefore, when multiplying from 1 to $p-1$ modulo p, all of the inverse pairs cancel out except for $(p-1, p-1)$ since there is only one instance of $p-1$. Therefore, if p is prime then $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

For the only-if direction, assume for the sake of contradiction that p is composite. We fix a prime factor q of p and notice that $(p-1)! \equiv 0 \pmod{q}$ since q must be a factor of $(p-1)!$. Therefore, $(p-1)!$ cannot have a residue of $p-1 \pmod{q}$ since $q \not| p-1$, contradicting our initial claim. $\square$

4 Fermat's Little Theorem

From Fermat's Little Theorem, we have that $n^7 - n \equiv 0 \pmod 7$, so all that is left to prove is that $n^7 - n \equiv 0 \pmod 6$.

Divide 6 into 2 and 3. Then, from more applications of Fermat, we find that $n^2 \equiv n \pmod 2$ and $n^2 \equiv 1 \pmod 3$. Therefore, modulo 2, we have $n^7 \equiv (n^2)(n^2)(n^2)(n) \equiv n^4 \equiv (n^2)(n^2) \equiv n^2 \equiv n \pmod 2$. Modulo 3, we have $n^7 \equiv (n^2)^3(n) \equiv n \pmod 3$. Therefore, $n^7 - n \equiv 0 \pmod 2$ and $n^7 - n \equiv 0 \pmod 3$ so $n^7 - n \equiv 0 \pmod 6$. □

5 Euler Totient Function

a) $\varphi(p) = p - 1$ because all positive integers $k < p$ are relatively prime to p, and there are $p - 1$ such integers.

b) $\varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}$. Take the $p^k - 1$ numbers less than p^k and remove the $p^{k-1} - 1$ multiples of p.

c) We observe that if there is a residue k modulo m such that $\gcd(k, m) = 1$, then $\gcd(k + am) = 1$ for all $a \in \mathbb{Z}$. Then, let the set M be the set of residues k modulo m such that $\gcd(k, m) = 1$, and the set N be the set of residues k modulo n such that $\gcd(k, n) = 1$.

Then, from the Chinese Remainder Theorem, since $\gcd(m, n) = 1$, then there is one x modulo mn that satisfies $x \equiv p \pmod{m}, x \equiv q \pmod{n}$. Therefore, for every $p \in M, q \in N$, there is one such x. Therefore, $\varphi(mn) = |M||N| = \varphi(m)\varphi(n)$. □

d) Let's observe every prime factor separately. For $x = p_i^{\alpha_i}$, we have $\varphi(x) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ from part (b). As we know from part (c) that φ is multiplicative, we find that

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i} - p_i^{\alpha_i - 1}.$$

Simplifying gives us

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1).$$

$$\implies \varphi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

□

6 Euler's Totient Theorem

a) If $f(x) = ax \mod n$ is not a bijection, we have two values m_i, m_j such that $am_i \equiv am_j \pmod{n}$. Since $\gcd(a, n) \equiv 1$, we can multiply both sides by a^{-1} to get $am_i a^{-1} \equiv am_j a^{-1} \pmod{n} \implies m_i \equiv m_j \pmod{n}$. Therefore, all am_i must map to a distinct value, or in other words, f is a bijection. □

b) From (a), we know that $\{am_1, am_2, \ldots, am_{\varphi(n)}\}$ is a permutation of $\{m_1, m_2, \ldots, m_{\varphi(n)}\}$. Therefore, we have that

$$\prod_{i=0}^{\varphi(n)} m_i \equiv \prod_{i=0}^{\varphi(n)} am_i \pmod{n}.$$

The RHS evaluates to

$$a^{\varphi(n)} \prod_{i=0}^{\varphi(n)} m_i \pmod{n},$$

and as $\prod_{i=0}^{\varphi(n)} m_i$ is coprime to n by definition we can multiply by its inverse, giving us $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

7 Sparsity of Primes

Let's think of $x+i$ in terms of being divisible by the product of two primes. Therefore, for each $x+i$, we would want $x+i \equiv 0 \pmod{p_{2i-1}p_{2i}}$ for all $i \in [1,k]$. Reducing to make the relations in terms of x, we have $x \equiv -i \pmod{p_{2i-1}p_{2i}}$. We can come up with $2k$ distinct primes because there are infinite primes. This means all p_i are distinct, so the moduli are all coprime. We have reduced the claim to k modular equations with k coprime moduli, so from the Chinese Remainder Theorem there must exist an x such that $x+1, x+2, \ldots, x+k$ are all not prime powers. $\square$

8 Sundry

Consulted Yuchan Yang for help with problem 7.