MATH 2170-19W Problem Set 4

March 1, 2019

Solutions

Question 1.

[2] (a) Let $m > 1$ be an odd natural number. Prove that

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (m-2) \equiv (-1)^{\frac{m-1}{2}} \cdot 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (m-1) \pmod{m}$$

[Hint: $1 \equiv -(m-1) \pmod{m}$, $3 \equiv -(m-3) \pmod{m}$, $\ldots$, $m-2 \equiv -2 \pmod{m}$]

Proof: This is just a re-naming of all the factors in the left hand component according to the hint. There are $\frac{m-1}{2}$ factors. So:

$$\begin{aligned} 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (m-2) &\equiv [-(m-1)][-(m-3)] \cdot \ldots \cdot (-4)(-2) \\ &\equiv (-1)^{\frac{m-1}{2}}[(m-1)(m-3) \cdot \ldots \cdot 4 \cdot 2] \\ &\equiv (-1)^{\frac{m-1}{2}} \cdot 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (m-1) \pmod{m} \end{aligned}$$

∎

[4] (b) If p is an odd prime, prove that

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \equiv 2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \pmod{p}$$

[Hint: Use Part (a), and rearrange the Wilson's Theorem formula in two different ways.]

Proof: By Wilson's Theorem, $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{p}$. Grouping together first all the odd factors and then all the even factors, we get

$$[1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2)] \cdot [2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)] \equiv -1 \pmod{p}.$$

We can simplify this in two ways by part (a), either by converting the first group of factors to the second; or by converting the second group to the first.

So in the first case we get

$$[(-1)^{\frac{p-1}{2}} \cdot 2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)] \cdot [2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1)] \equiv -1 \pmod{p},$$

which after grouping similar factors and gathering powers of (-1) gives

$$2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

If we make the alternate conversion, we get the other part of the formula that we were supposed to prove. ∎

[2] **Question 2.** Take note that $17 = 1^2 + 4^2 = 4^2 + 1^2$ and $13 = 2^2 + 3^2$

Write $221 = 13 \cdot 17$ as a sum of two squares in two different ways.

Solution: We have

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

The "Note" indicates we should work this out in two ways, taking first $a = 1,\ b = 4$ and $c = 2\, d = 3$ and in the second case $a = 1,\ b = 4$ and $c = 3\, d = 2$.

We get

$$221 = (2 - 12)^2 + (3 + 8)^2 = 10^2 + 11^2$$
$$221 = (8 - 3)^2 + (12 + 2)^2 = 5^2 + 14^2$$

[4] **Question 3.** Write each of the following as a sum of two squares.

(a) 1960 (b) $121,000$

Solution: There are quite a few different pathways to a correct solution. I think that this is the most efficient. You did have to give some sort of explanation here of how you found your answer.

(a) $1960 = 2^3 3^7 5 = (2 \times 7)^2 \times 10$, and $10 = 1^2 + 3^2$. So $1960 = 14^2 + 42^2$ ../

(b) $121000 = 11^2 \times 10^3 = (11 \times 10)^2 \times 10$. $10 = 1^2 + 3^2$. So $121000 = (110 \times 1)^2 + (110 \times 3)^2 = 110^2 + 330^2$

[4] **Question 4.** Solve $55x \equiv 91 \pmod{108}$ by solving a pair of congruences, one modulo 4, the other modulo 27.

Solution: So if $55x \equiv 91 \pmod{108}$ then $3x \equiv 3 \pmod 4$ and $x \equiv 10 \pmod{27}$. So $x \equiv 1 \pmod 4$.

Furthermore, $x = 10 + 27t$ for some t. Therefore $10 + 27t \equiv 1 \pmod 4$, or $3t \equiv 3 \pmod 4$. So $t \equiv 1 \pmod 4$ and for some s, $t = 1 + 4s$.

Therefore $x = 10 + 27(1 + 4s) = 37 + 108s$.

The unique solution modulo 108 is $x \equiv 37 \pmod{108}$.

[4] **Question 5.** Find the smallest positive integer solution to

$$\begin{aligned} x &\equiv 3 \pmod{14} \\ x &\equiv 4 \pmod{15} \\ x &\equiv 5 \pmod{11} \end{aligned}$$

Solution: I prefer to start with the largest modulus for reasons of computational efficiency, but any order will work.

So $x = 4 + 15r$ for some r.

Therefore $4 + 15r \equiv 3 \pmod{14}$, or $r \equiv -1 \equiv 13 \pmod{14}$.

Thus $r = 13 + 14s$ for some s, so $x = 4 + 15(13 + 14s) = 199 + 210s$.

Therefore $199 + 210s \equiv 5 \pmod{11}$, or $1 + s \equiv 5 \pmod{11}$, so $s \equiv 4 \pmod{11}$.

Thus $s = 4 + 11t$ for some t, so $x = 199 + 210(4 + 11t) = 1039 + 2310t$.

There is a unique solution modulo $2310 = 14 \times 15 \times 11$, namely $x \equiv 1039 \pmod{2310}$.