EXCEL 21-127

20, 21 April 2020

1. **Let x, y be integers satisfying $x^4 + x^2 = 8y$. Show that $4 \mid x$.**

Consider x modulus 4,

0	$x^4 + x^2 \equiv 0 \bmod 8$
1	$x^4 + x^2 \equiv 2 \bmod 8$
2	…

$x^2(x^2+1) = 8y$, so $8 \mid x^2(x^2+1)$

Claim: x cannot be odd, because 8 does not divide $x^2 + 1$

If $x = 2k+1$ then $x^2 + 1 = 4k^2 + 4k + 2 = 4s + 2$

Therefore, $8 \mid x^2$

AFSOC $x \equiv 2 \bmod 4$ then $x = 4k + 2$ so $x^2 = 16k^2 + 16k + 4$

2. **Show that if p and $p^2 + 2$ are both primes, so is $p^3 + 2$.**

Only prime $p = 3$ satisfies $p^2 + 2$ is prime.

For any prime $p \neq 3$, $p^2 + 2 \equiv 0 \bmod 3$.

3. **Show that $n^7 - n$ is divisible by 42 for every positive integer n.**

Want to show $42 \mid n^7 - n = n(n^6 - 1) = n(n^3+1)(n^3-1)$

Want to show $2 \mid n^7 - n$ and $3 \mid n^7 - n$ and $7 \mid n^7 - n$

n and $n^3 + 1$ must have different parity, so $2 \mid n(n^3+1)$

If $n \equiv 1 \bmod 3$, then $3 \mid n^3 - 1$; if $n \equiv 2 \bmod 3$, then $3 \mid n^3 + 1$

Consider n modulus 7,

0	$7 \mid n$
1	$7 \mid n^3 - 1$

2	$7 \mid n^3 - 1$
3	$7 \mid n^3 + 1$
4	$7 \mid n^3 - 1$
5	$7 \mid n^3 + 1$
6	$7 \mid n^3 + 1$

For case $n \equiv 1 \bmod 7$: $n^3 - 1 \equiv 1^3 - 1 \equiv 0 \bmod 7$

For case $n \equiv 5 \bmod 7$: $n^3 + 1 \equiv 5^3 + 1 \equiv 125 + 1 \equiv 126 \equiv 0 \bmod 7$

Lemma 1.

If $x \equiv y \bmod n$, then $x^k \equiv y^k \bmod n$.

Want to show $n \mid x^k - y^k = (x - y) \cdot A$

Lemma 2.

If $a \mid n$ and $b \mid n$ then $ab \mid n$, only true if $\gcd(a, b) = 1$.

$n = ak$, but $b \mid n$ so $b \mid ak$; since b does not divide a, so $b \mid k$, that is $k = bk'$, so $n = abk'$

4. **Fix modulus n. Prove or disprove for all integers a, b, q and $q \neq 0 \bmod n$ we have $qa \equiv qb \rightarrow a \equiv b$.**

$$n \mid qa - qb = q(a - b) \rightarrow n \mid (a - b)$$

Counterexample: $a = 5, b = 7, q = 3, n = 6$

5. **Let p be a prime. Find $\gcd\big((p - 1)! + 1, p!\big)$.**

Let $\gcd\big((p - 1)! + 1, p!\big) = x$. Then x does not divide $(p - 1)!$

$p \mid (p - 1)! + 1$ by Wilson's theorem

Lemma: $\gcd(n, n + 1) = \gcd(n, 1) = 1$

6. **Show that $n^5 - n$ is divisible by 30 for every positive integer n.**
7. **Show that 4 does not divide $n^2 + 2$ for any positive integer n.**

8. **Show that for every positive integer n we have $\sum_{i=1}^{n} i^3 \mid 3 \cdot \sum_{i=1}^{n} i^5$.**

$3 \cdot ? \equiv 1 \bmod 12$

$3 \cdot ? \equiv 1 \bmod 13$

$13k = 3 \cdot ? - 1$, that is, $3 \cdot ? + 13 \cdot (-k) = 1$

$\gcd(x, y) = n$, then extended Euclidean algorithm gives a, b such that $ax + by = n$.

9. **Find x such that $2x + 9 \equiv 3x + 7 \bmod 5$.**

$x \equiv 2 \bmod 5$.

$$5 \mid (2x + 9) - (3x + 7)$$

$$5 \mid 2 - x$$

10. **Find x such that $25x - 4 \equiv 4x + 3 \bmod 13$.**

$21x \equiv 7 \bmod 13$ (we can also divide both side by 7, so $3x \equiv 1 \bmod 13$.)

$8x \equiv 7 \bmod 13$

Want to find $8x - 7 = 13k$, that is $8x - 13k = 7$

$8a + 13b = 1$ for some a, b

$a = 5, b = -3$. That is, $8 \cdot 5 - 13 \cdot 3 = 1$ so $x = 5 \cdot 7 \equiv 9 \bmod 13$.