Math 320 - Dr. Miller - Exam #3, Fall 2015 - Monday, Nov. 23, 2015 - **Fibonacci Day!** 88 88 = 100%

1. *[15 pts]* Find ALL Pythagorean triples (including non-primitive) that involve the number 20. Show work, but you need not explain anything verbally.

2. *[6 pts]* Is there a number $n \in \{30, 31, 32, \ldots, 40\}$ that cannot occur in a PRIMITIVE Pythagorean triple? Justify your claim, including a sentence of explanation.

3. (a) *[5 pts]* Precisely define the Euler phi-function $\phi(n)$, including hypotheses.
   (b) *[4 pts]* Compute $\phi(555)$, writing your answer in ordinary whole number notation.
   (c) *[4 pts]* Compute $\phi(3^{19} \cdot 5^{100} \cdot 19^{40})$, writing your answer in prime factored form.

4. *[17 pts]* Precisely state Wilson's Theorem, then prove its converse.

5. *[8 pts]* Give an example of a Mersenne prime and of a Fermat prime, telling which is which and making clear their defining features.

6. ~~*[12 pts]* Let p be a prime number and $a \in \mathbf{Z}^+$ such that $a \nmid p-1$. Prove that ap divides $(p-1)! + a^a$.~~ Deleted

p-1|a and (a,p)=1

7. *[17 pts]* Precisely state Fermat's Little Theorem, then PROVE it for the case where the modulus is 13 and the other number is 2. (Note: I am not asking you to APPLY FLiT; rather, you have to reproduce the actual proof using my values.)

8. *[12 pts]* Evaluate 3^{277} mod 91. Show work/justification.

82.4% med.

320 - Exam #3, Fall 2015

(15) 1. Find primitive triples involving 1, 2, 4, 5, 10, 20

3 each with work

1 - not possible (y is even, + no squares have a difference or sum of 1)

2 - not possible ($y = 2mn = 2 \Rightarrow m = n = 1$, same parity)

4 - $y = 2mn = 4$ means $m = 2, n = 1$

$x = 2^2 - 1^2 = 3$

$z = 2^2 + 1^2 = 5$

$(3,4,5) \times 5 = \boxed{(15, 20, 25)}$

5 - $x = 5 = m^2 - n^2$ means $m = 3, n = 2$

$y = 2 \cdot 3 \cdot 2 = 12$

$z = 3^2 + 2^2 = 13$

$(5,12,13) \times 4 = \boxed{(20, 48, 52)}$

(-2) discarded instead of scaled.

or $z = 5 = m^2 + n^2$ means $m = 2, n = 1$

so

$(3,4,5) \times 4 = \boxed{(12, 16, 20)}$

continuing with m=5, n=1 would create a triple but it will be one that already is creatable from earlier primitives, so unnecessary.

10 - $y = 10 = 2mn$ means $m = 5, n = 1$
same parity

Not possible

20 - $y = 20 = 2mn$ means $m = 10, n = 1$
$x = 10^2 - 1^2 = 99$
$z = 10^2 + 1^2 = 101$

$\boxed{(99, 20, 101)}$

(or) $y = 20 = 2mn$ means $m = 5, n = 2$
$x = 5^2 - 2^2 = 21$
$z = 5^2 + 2^2 = 29$

$\boxed{(21, 20, 29)}$

---

(6) a. 30 cannot occur:
if it did, it would have to be that
$y = 30$, whence $2mn = 30$
and $mn = 15$.
But then m and n must both be odd,
a contradiction.

-1) reference to x, z.

-3) $m \equiv n \bmod 2$ is believed to work.

(34 and 38 create this same misadventure!)
in parity

(Note that any odd # greater than 1 always occurs, for the seq. of squares has difference seq. $2n+1$)

13

-1 imprecision
-2 $\varphi(n)$ is a set, not a formula, not defn.
-3 no hypoth.

3.a. (5) For $n \in \mathbb{Z}^+$ (1), $\varphi(n)$ is the number of positive (1) integers less than or equal to n that are relatively prime to n.

b. (4) $555 = 5 \cdot 111 = 5 \cdot 3 \cdot 37$

So $\varphi(555) = \varphi(3) \cdot \varphi(5) \cdot \varphi(37)$

$= (3-1) \cdot (5-1) \cdot (37-1)$

$= 2 \cdot 4 \cdot 36$

$\boxed{= 288}$

-1 not HW form

c. (4) $n = 3^{19} \cdot 5^{100} \cdot 19^{40}$ with prime divisors 3, 5, 19

-2 not prime fact. not simplified fraction

$$\varphi(n) = n \cdot \prod_{\substack{\text{primes } p, \\ p \mid n}} \left(1 - \frac{1}{p}\right)$$

$$= 3^{19} \cdot 5^{100} \cdot 19^{40} \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{19}\right)$$

$$= 3^{19} \cdot 5^{-100} \cdot 19^{40} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{18}{19}$$

$$= 3^{18} \cdot 5^{99} \cdot 19^{39} \cdot 2 \cdot 2^2 \cdot 2 \cdot 3^2$$

$$\boxed{= 2^4 \cdot 3^{20} \cdot 5^{-99} \cdot 19^{39}}$$

17

4. (5) Wilson's Theorem - Let p be prime. Then $(p-1)! \equiv -1 \bmod p$.

Converse: If $(p-1)! \equiv -1 \bmod p$, then p is prime

(+1) modulus $=1$ issue

(+0) no $n>0$ restriction

(-1) bad $a<n$ reasoning

(-2) $a<b$ (trivial but one portion)

(-3) assume $a<n$.

Proof (by ctp) (as HW) - Suppose p is not prime, but composite ($p=1$, a unit, would create a counterexample).

Then we know p can be written as $p = ab$ where $1 < a, b < p$.

If $a \neq b$, then both occur separately as factors in $(p-1)!$, whence $ab \mid (p-1)!$, but $ab = p$. So $(p-1)! \equiv 0 \bmod p$, and $p \neq 1$ implies $0 \not\equiv -1 \bmod p$.

Thus $(p-1)! \not\equiv -1 \bmod p$ in this case.

If $a = b$ and $p > 4$, then as a perfect square, $p \geq 9$ and $a = b \geq 3$. Thus $2a < 3a \leq ba = p$, so $2a \leq p-1$; therefore, a and $2a$ are distinct factors of $(p-1)!$, whence $a^2 \mid (p-1)!$, but $a^2 = p$, so again $(p-1)! \equiv 0 \bmod p$, and the case concludes as above.

If $p = 4$, then $(p-1)! = 3! = 6 \not\equiv -1 \bmod 4$.

Thus, if p is not prime, then $(p-1)! \not\equiv -1 \bmod p$.

---

(8) 5. (4) Mersenne prime: 31, because it's of the form $2^n - 1$ ($n = 5$ in this case)

(4) Fermat prime: 17, for it is of the form $2^{2^k} + 1$ (where $k = 2$: $2^{2^2} + 1 = 2^4 + 1 = 16 + 1$)

(#4) Variation

Proof (direct) (as in book) – Suppose $(p-1)! \equiv -1 \bmod p$ and $p = ab$ with $a, b \in \mathbb{Z}^+$.
So $a \mid p$ and also $p \mid (p-1)! + 1$
Thus $a \mid (p-1)! + 1$.
Also without loss of generality, let $a \leq b$.
So $a < p$, else $p = p^2$, whence $p = 1$ (which we cannot allow, else a counterexample would occur).
Then $a \mid (p-1)!$, so a divides 1, which is a linear combination of $(p-1)! + 1$ and $(p-1)!$.
But then a must equal 1, making p prime.

---

(5) 6. Deleted – untrue

---

(17) 7. FLiT, Fermat's Little Theorem –
5 Let p be prime and $(a, p) = 1$ (or $p \nmid a$). Then $a^{p-1} \equiv 1 \bmod p$.

-2 lost $(a,p)=1$

-2 lost p prime.

12

Proof for $p=13$, $a=2$: Consider the values $2, 4, 6, \ldots, 12 \cdot 2 = 24$. of the form $2i$ where $i = 1, 2, \ldots, 12$.

None are congruent to 0 mod p, for $13 \mid 2i$ implies $13 \mid 2$, an impossibility or $13 \mid i$, also impossible due to their size.

Mod 13, these values are distinct, for $2i \equiv 2j \bmod 13$ implies $i \equiv j \bmod 13$ (divide by 2), but i, j are viable remainders mod 13, so then $i = j$.

Thus these 12 numbers are congruent mod 13 to the 12 numbers $1, 2, \ldots, 12$ in some order.

So $\prod_{i=1}^{12} (2i) = 2^{12} \cdot \prod_{i=1}^{12} i = 2^{12} \cdot 12!$

is congruent mod 13 to $12!$.

By Wilson's Theorem, we have $12! \equiv -1 \bmod 13$.

So $2^{12} \cdot 12! \equiv 12! \bmod 13$

means $-2^{12} \equiv -1 \bmod 13$

and $2^{12} \equiv 1 \bmod 13$,

as desired.

-9 computational confirmation.

-2 numerical confirmation only

-2 no proof of distinct residues mod 13.

-2 no proof of residue-ness

-1 ref to theorem, not residue

-4 tangled/incomplete "equation"

(12) 8. $3^{277} \bmod 91 = 7 \cdot 13$

FLiT approach: (variations are many!)

$3^{12} \equiv 1 \bmod 13$ and $3^6 \equiv 1 \bmod 7$

$$3^{277} = (3^{12})^{23} \cdot 3 \equiv 1 \cdot 3 = 3 \bmod 13$$

$$3^{277} = (3^6)^{46} \cdot 3 \equiv 1 \cdot 3 = 3 \bmod 7.$$

Since $3^{277} \equiv 3 \bmod 13$ and $\bmod 7$, with $(13, 7) = 1$, uniqueness in the CRT implies that $\boxed{3^{277} \equiv 3 \bmod 91}$

(-7) assumed $3^{90} \equiv 1$

(-2) $3^{\text{appro}} \equiv -1$.

(-4) inappropriate exponents for modulus 7, 13

(-3) each independent sig. error

(-2)

Euler's Theorem approach:

$(3, 91) = 1$ and $\varphi(91) = \varphi(7) \cdot \varphi(13)$

$= 6 \cdot 12 = 72$,

so $3^{\varphi(91)} = 3^{72} \equiv 1 \bmod 91$

$$3^{277} = (3^{72})^3 \cdot 3^{61} \equiv 1 \cdot 3^{61} \bmod 91$$

also $3^6 \equiv 1 \bmod 91$ since $3^6 = 729$ and $91 \times 8 = 728$

so $3^{61} = (3^6)^{10} \cdot 3 \equiv 1 \cdot 3 \boxed{= 3 \bmod 91}$

"Brute force" approach: note above $3^6 \equiv 1 \bmod 91$

$$3^{277} = (3^6)^{46} \cdot 3 \equiv 1 \cdot 3 \boxed{= 3 \bmod 91}$$