Review for Exam 2

#1 g) $\boxed{3}$ #2

f) $\boxed{11}$

b-d) $\boxed{0}$

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

#4) $7\overline{)436}$ 62 R2

$7\overline{)2345}$ 335 R0

$2 \times 0 = \boxed{0}$

#5) $4^{5042} \bmod 5 = (-1)^{5042} \bmod 5 = \boxed{1}$

$4^1 = 4$

$4^2 = 16 \to 1$

$4^3 = 4$

$4^4 = 16 \to 1$

$4^{\text{even}} = 1 \pmod 5$

Another way

$\underbrace{4 \times 4}_{16} \times \underbrace{4 \times}_{16} \cdots \underbrace{\quad}_{16} \times \underbrace{4 \times 4}_{16}$

$1 \quad 1 \quad 1 \quad 1 = 1$

#7

32	51
64	102
96	153
128	204
⋮	255
256	

Aha

#6

$51 = 1\cdot 32 + 19$

$32 = 1\cdot 19 + 13$

$19 = 1\cdot 13 + 6$

$13 = 2\cdot 6 + \boxed{1}$ gcd = 1

$6 = 6\cdot 1 + 0$

Unfold:

$1 = 13 - 2\cdot 6$

$= 13 - 2\cdot(19 - 1\cdot 13) = 3\cdot 13 - 2\cdot 19$

$= 3\cdot(32 - 1\cdot 19) - 2\cdot 19 = 3\cdot 32 - 5\cdot 19$

$= 3\cdot 32 - 5(51 - 1\cdot 32) = 8\cdot 32 - 5\cdot 51$

You have to do this until you can do it!

So... $32^{-1} = \boxed{8}$

#10) $\varphi(17) = 16$

#11) $\varphi(2025) = \varphi(5^2 \cdot 3^4) = (5^2 - 5^1)\cdot(3^4 - 3^3) = 1080$

#12) F.L.T If p is prime and n, p rel. prime, then $n^{p-1} \bmod p = 1$.

So $7^{10} \bmod 11 = \boxed{1}$

~~$7^9 \bmod 11 = 1 \longrightarrow ???$~~

#13) $a^{\varphi(n)} \bmod n = 1$

as long as $\gcd(a,n) = 1$.

On the final

There will be a +10 XC opportunity for mastering the material of page 5 of Exam 2.

More Logic: Negating Compound Propositions

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \wedge \neg q) \equiv \neg p \vee \neg\neg q \equiv \neg p \vee q$$

$$\neg((p \to q) \wedge (p \oplus r)) \equiv \neg(p \to q) \vee \neg(p \oplus r)$$

Not done yet!

Not done until there are no further compound negations.

I.e. the only negated expressions are simple propositions ($\neg p, \neg q, \neg r, \ldots$)

$$\equiv \boxed{(p \wedge \neg q) \vee (p \Leftrightarrow r)}$$

$$\neg\big((p \to q) \oplus (r \land (\neg s \to t))\big)$$

$$\equiv (p \to q) \Longleftrightarrow (r \land (\neg s \to t))$$

$$\boxed{\neg(p \oplus q) \equiv p \Longleftrightarrow q} \qquad \boxed{\neg(p \to q) \equiv p \land \neg q}$$

$$\neg\big((p \land r) \Rightarrow (s \lor t)\big) \equiv (p \land r) \land \neg(s \lor t)$$

$$\equiv (p \land r) \land (\neg s \land \neg t)$$

Done . . .