

Put your answers in the space provided. Show your reasoning. Calculators are to be used when appropriate. The maximum score on the test is 30 points.

1. 4 points Without using your calculator find the remainder when 2007^{2007} is divided by 13.

$$2007 \equiv 707 \equiv 57 \equiv 5 \pmod{13} \qquad 2007 \equiv 807 \equiv 87 \equiv 3 \pmod{12}$$

$$2007^{2007} \equiv 5^{12 \cdot s + 3} \equiv (5^{12})^s \cdot 5^3 \equiv 1^s \cdot 25 \cdot 5 \equiv -5 \equiv 8 \pmod{13}$$

So the remainder is 8

2. 4 points Find the two smallest positive solutions to

$$2x \equiv 8 \pmod{4} \qquad 3x \equiv 9 \pmod{5} \qquad 4x \equiv 10 \pmod{6}$$

Our system is equivalent to

$$x \equiv 0 \pmod{2} \qquad x \equiv 3 \pmod{5} \qquad x \equiv 1 \pmod{3}$$

$$\text{So } x = 2a \qquad 2a \equiv 3 \equiv 8 \pmod{5} \qquad a \equiv 4 \pmod{5} \qquad a = 4 + 5b$$

$$x = 2(4 + 5b) = 8 + 10b \qquad 8 + 10b \equiv 1 \pmod{3} \qquad b \equiv -7 \equiv 2 \pmod{3}$$

$$b = 2 + 3c$$

$$x = 8 + 10(2 + 3c) = 28 + 30c$$

The two smallest positive solutions are 28 and 58

3. 3 points Theorem: If $a|c$ and $b|c$ and if $(a, b) = 1$, then $ab|c$

Proof:

1.	$c = as, c = bt$	definition of division
2.	$ax + by = 1$ for some x, y	Since $(a, b) = 1$
3.	$cax + cby = c$	Multiply both sides by c
4.	$btax + asby = c$	substitute from 1.
5.	$ab(tx + sy) = c$	ROF, factor out ab
6.	$ab c$	definition of division

In the boxes fill in a short reason for that step. An acceptable reason is ROA (rules of algebra).

4. 4 points Characterize those positive integers n for which $\frac{\phi(n)}{2}$ is odd. Clearly indicate your answer.

$$\frac{\phi(4)}{2} = 1. \text{ If } n = p^\alpha \text{ for some odd prime } p, \text{ then } \phi(n) = n \left(1 - \frac{1}{p}\right) = n \left(\frac{p-1}{p}\right).$$

So if $\frac{\phi(n)}{2}$ is odd, 4 does not divide $p-1$ or $p \equiv 3 \pmod{4}$

$$\phi(2) = 1. \qquad \text{So if } (n, 2) = 1, \text{ then } \phi(2n) = \phi(n)$$

$n = 4$ or if $n = p^\alpha$ or $n = 2p^\alpha$ with p prime and $p \equiv 3 \pmod{4}$, then $\frac{\phi(n)}{2}$ is odd.

5. 4 points Let p be a prime number. Prove that if $m = 2^p - 1$ is a composite number, then m is a pseudoprime number.

Since p is prime, $2^p \equiv 2 \pmod{p}$; i.e. $p \mid 2^p - 2$. We know that if $m \mid n$, then $2^m - 1 \mid 2^n - 1$, so $2^p - 1 \mid 2^{2^p - 2} - 1$. Consequently $2^p - 1 \mid 2 \cdot (2^{2^p - 2} - 1) = 2^{2^p - 1} - 2$ or $2^m \equiv 2 \pmod{m}$.

Since m is composite, it is a pseudoprime.

6. 4 points Prove: If $(a, b) = 1$, and $(a, c) = 1$, then $(a, bc) = 1$

$$\begin{aligned} ax + by = 1 \text{ and } at + cs = 1 \text{ so } 1 &= (ax + by)(at + cs) = a^2xt + axcs + byat + bcys = \\ &= a(axt + cxs + byt) + bc(ts) \end{aligned}$$

$$\text{So } (a, bc) = 1$$

7. 4 points Use Wilson's Theorem to find the remainder when $2(26!)$ is divided by 29

$$\text{We know that } 27! \equiv 27 \cdot 26! \equiv -2 \cdot 26! \equiv 1 \pmod{29}$$

$$\text{So } \boxed{2(26!) \equiv -1 \equiv 28 \pmod{29}} \text{ or } \boxed{\text{the remainder is 28}}$$

8. 3 points Use Fermat's Theorem to show that for any prime p and integers a and b ,

$$\boxed{(a + b)^p \equiv a^p + b^p \pmod{p}}$$

Using Fermat's Little Theorem three times we have $a \equiv a^p \pmod{p}$, $b \equiv b^p \pmod{p}$

$$\boxed{(a + b)^p \equiv a + b \equiv a^p + b^p \pmod{p}}$$