MATH 580/780I: TEST 2, FALL 2010

Instructions and Point Values: Put your name at the top of the first page of the blank paper given to you. There are 6 problems below. Work each problem on the paper provided, using a separate page for each problem. Circle your answer (not the work) on the blank page for each part of each problem. Show ALL of your work. Do NOT use a calculator.

There are 100 total points possible on this exam. The point value for each problem appears to the left of each problem.

---

18 pts (1) Calculate each of the following. Simplify your answers. Each part of this problem should have a short solution based on a theorem or formula from class.

(a) The value of $\phi(2^2 \cdot 3^2 \cdot 5)$.

(b) The smallest positive integer a such that $9^{12} \equiv a \pmod{13}$.

(c) An integer b between -100 and 100 satisfying $12! \equiv b \pmod{13}$.

(a) $\boldsymbol{\phi(2^2 \cdot 3^2 \cdot 5) = \phi(2^2) \cdot \phi(3^2) \cdot \phi(5) = (2^2 - 2)(3^2 - 3)(5 - 1) = 2 \cdot 6 \cdot 4 = \boxed{48}}$

(b) Since $\gcd(9, 13) = 1$, we obtain from Fermat's Little Theorem that $9^{12} \equiv \boxed{1} \pmod{13}$.

(c) By Wilson's Theorem, $12! \equiv \boxed{-1} \pmod{13}$.

---

18 pts (2) (a) Define the word "pseudoprime".

(b) Prove that each of the following congruences is valid.

$$2^{40} \equiv 1 \pmod{3}, \quad 2^{40} \equiv 1 \pmod{11}, \quad 2^{40} \equiv 1 \pmod{17}, \quad 2^{40} \equiv 1 \pmod{41}$$

(c) Using part (b), explain why $23001 = 3 \cdot 11 \cdot 17 \cdot 41$ is a pseudoprime. You should be able to handle all the cases (each prime) at once.

(a) A *pseudoprime* is a composite number n satisfying $2^n \equiv 2 \pmod{n}$.

(b) $\boldsymbol{2^2 \equiv 1 \pmod{3} \implies 2^{40} \equiv (2^2)^{20} \equiv 1^{20} \equiv 1 \pmod{3}}$
$\boldsymbol{2^{10} \equiv 1 \pmod{11} \implies 2^{40} \equiv (2^{10})^4 \equiv 1^4 \equiv 1 \pmod{11}}$
$\boldsymbol{2^4 \equiv -1 \pmod{17} \implies 2^{40} \equiv (2^4)^{10} \equiv (-1)^{10} \equiv 1 \pmod{17}}$
$\boldsymbol{2^{40} \equiv 1 \pmod{41}}$

Note that for the moduli 3, 11 and 41, Fermat's Little Theorem has been used to obtain the first congruence mentioned. For the modulus 17, one gets directly that $2^4 \equiv 16 \equiv -1 \pmod{17}$.

(c) From part (b), we know that $2^{40} - 1$ is divisible by each of 3, 11, 17 and 41. Since 3, 11, 17 and 41 are pairwise relatively prime, we deduce that $2^{40} - 1$ is divisible by $23001 = 3 \cdot 11 \cdot 17 \cdot 41$. Therefore, $2^{40} \equiv 1 \pmod{23001}$, and we obtain

$$\boldsymbol{2^{23000} \equiv (2^{40})^{575} \equiv 1^{575} \equiv 1 \pmod{23001} \implies 2^{23001} \equiv 2 \pmod{23001}.}$$

Since $23001 = 3 \cdot 11 \cdot 17 \cdot 41$ is composite, we deduce that 23001 is a pseudoprime.

$\boxed{\text{20 pts}}$ (3) (a) State Euler's Theorem.

(b) Calculate $\phi(1000)$.

(c) Give a one sentence explanation for why Euler's Theorem does NOT imply

$$2^{\phi(1000)} \equiv 1 \pmod{1000}.$$

(d) What is the remainder when $2^{\phi(1000)}$ is divided by 1000? In other words, determine what $R \in \{0, 1, 2, \dots, 999\}$ satisfies $2^{\phi(1000)} \equiv R \pmod{1000}$.

(a) If a and n are integers with $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(b) $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3) \cdot \phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = \boxed{400}$.

(c) Euler's Theorem does not apply since $\gcd(2, 1000) = 2 \neq 1$.

(d) Letting $x = 2^{\phi(1000)} = 2^{400}$ (where the last equation comes from part (b)), we see that

$$x \equiv 2^{400} \equiv 0 \pmod{2^3}.$$

Since $\phi(5^3) = 5^3 - 5^2 = 100$ and $\gcd(2, 5^3) = 1$, we obtain from Euler's Theorem that

$$2^{100} \equiv 1 \pmod{5^3} \implies x \equiv 2^{400} \equiv (2^{100})^4 \equiv 1^4 \equiv 1 \pmod{5^3}.$$

Hence, we have $x \equiv 0 \pmod{2^3}$ and $x \equiv 1 \pmod{5^3}$. Observe that the inverse of $2^3 = 8$ modulo $5^3 = 125$ is 47 since $3 \cdot 125 + 1 = 376 = 8 \cdot 47$. From our approach to solving simultaneous linear congruences (i.e., the Chinese Remainder Theorem), we deduce

$$x \equiv 1 \cdot 2^3 \cdot 47 \equiv 376 \pmod{1000}.$$

So the remainder is $\boxed{376}$.

$\boxed{\text{12 pts}}$ (4) Find the smallest positive integer n satisfying all of the following:

- The number $n + 2$ is divisible by 2.
- The number $n + 20$ is divisible by 20.
- The number $n + 201$ is divisible by 201.
- The number $n + 2010$ is divisible by 2010.

Note that $n = 0$ is an "obvious" integer that satisfies the above four conditions. In the problem, I am asking for you to find the next n with this property. You may want to use that $201 = 3 \cdot 67$ and $2010 = 2 \cdot 3 \cdot 5 \cdot 67$.

Note that $n + k$ is divisible by k for some integer k if and only if $n + k = kt$ for some integer t. On the other hand, $n + k = kt$ if and only if $n = k(t - 1)$. So $n + k$ is divisible by k for some integer k if and only if k divides n. The smallest positive integer n satisfying the congruences in the problem is therefore the same as the smallest positive integer divisible by 2, 20, 201 and 2010. Since

$$2 = 2, \quad 20 = 2^2 \cdot 5, \quad 201 = 3 \cdot 67, \quad \text{and} \quad 2010 = 2 \cdot 3 \cdot 5 \cdot 67,$$

we see that n must be the first positive integer divisible by $2^2 \cdot 3 \cdot 5 \cdot 67 = 4020$ The answer is therefore $\boxed{4020}$.

12 pts (5) What is the remainder when

$$123456789101112\ldots9899100$$

is divided by 90? (The digits of the number displayed above are 1, 2, 3, ..., 100 written side-by-side.)

Let $x = 123456789101112\ldots9899100$. Since x ends in a 0, we have x is divisible by 10. Thus, $x \equiv 0 \pmod{10}$. Also,

$$x \equiv 1+2+3+\cdots+99+100 \equiv \frac{100\cdot 101}{2} \equiv 5050 \equiv 1 \pmod{9}.$$

Since $x \equiv 0 \pmod{10}$ and $x \equiv 1 \pmod{9}$, we get

$$x \equiv 1\cdot 10\cdot 1 \equiv 10 \pmod{90}.$$

Therefore, the remainder is $\boxed{10}$.

---

20 pts (6) (a) Find the smallest positive integer solution to the system of congruences below.

$$\begin{aligned} x &\equiv 4 \pmod{8} \\ x &\equiv 8 \pmod{12} \\ x &\equiv 12 \pmod{20} \\ x &\equiv 20 \pmod{42} \end{aligned}$$

Simplify your answer (do the arithmetic). This could be a "little" messy. Deal with it.

(b) Solve the system of congruences above. In other words, describe the complete set of integers x that have the property that each x in the set satisfies ALL of the congruences displayed in part (a).

(a) and (b) We make use of the notation $\iff$ for "if and only if" (or "is equivalent to") to rewrite the system of congruences:

$$x \equiv 4 \pmod{8}$$

$$x \equiv 8 \pmod{12} \iff x \equiv 2 \pmod{3} \text{ and } x \equiv 0 \pmod{4}$$

$$x \equiv 12 \pmod{20} \iff x \equiv 0 \pmod{4} \text{ and } x \equiv 2 \pmod{5}$$

$$x \equiv 20 \pmod{42} \iff x \equiv 0 \pmod{2},\ x \equiv 2 \pmod{3} \text{ and } x \equiv 6 \pmod{7}.$$

If $x \equiv 4 \pmod{8}$, then $x = 8k+4$ for some integer k so that $x \equiv 0 \pmod{2}$ and $x \equiv 0 \pmod{4}$. So we are left with wanting x that satisfy

$$x \equiv 4 \pmod{8}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 2 \pmod{5}, \quad \text{and} \quad x \equiv 6 \pmod{7}.$$

We deduce

$$\begin{aligned} x &\equiv 4\cdot 105\cdot 1 + 2\cdot 280\cdot 1 + 2\cdot 168\cdot 2 + 6\cdot 120\cdot 1 \\ &\equiv 420 + 560 + 672 + 720 \equiv 2372 \equiv 692 \pmod{840}. \end{aligned}$$

The answer to (a) is $\boxed{692}$ and the answer to (b) is $\boxed{x = 692 + 840k, \text{ where } k \in \mathbb{Z}}$.