18.781 Exam 1 Solutions - Fall 2008

Problem 1. (*Short answer; 4 pts each*) Unless asked otherwise, you are not required to show detailed work for these questions, and need only give a brief explanation.

(a) Evaluate $\phi(24)$ and $\phi(31)$.

Solution. Using the formula $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, we find

$$\phi(24) = 24 \cdot \frac{1}{2} \cdot \frac{1}{3} = \boxed{\mathbf{8}},$$
$$\phi(31) = 31 \cdot \frac{30}{31} = \boxed{\mathbf{30}}.$$

(b) If $7a - 38b = -2$, what can you conclude about the greatest common divisor (a, b)?

Solution. If we write $g = (a, b)$, then $g \mid (ax + by)$ for any linear combination. Thus $g \mid 2$, so $\boxed{\boldsymbol{g = 1} \text{ or } \mathbf{2}}$.

(c) Explain why the square of the Möbius function is the indicator function for squarefree numbers; i.e., show that

$$\mu(n)^2 = \begin{cases} 1 & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

Solution. By definition,

$$\mu(n)^2 = \begin{cases} \left((-1)^{\omega(n)}\right)^2 = 1 & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

(d) Is $61^{61} + 71^{71}$ a multiple of 11?

Solution. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$ for a prime p, so

$$61^{61} + 71^{71} \equiv 6^{1+6 \cdot 10} + 5^{1+7 \cdot 10} \equiv 6 + 5 \equiv 0 \pmod{11},$$

so the answer is $\boxed{\mathbf{Yes}}$.

(e) Find an integer $m > 1$ that guarantees that $a^m \equiv a \pmod{99}$ for any a satisfying $(a, 99) = 1$? Is there a value of m that works for *all* integers a?

Solution. Euler's Theorem states that $a^{\phi(n)} \equiv 1 \pmod{n}$ for all $(a, n) = 1$. We have $\phi(99) = 99 \cdot \frac{2}{3} \cdot \frac{10}{11} = 60$, so $\boxed{\boldsymbol{m = 61}}$.

As for the second question, this will be ignored in the grading as it was misstated and is rather subtle as written. For completeness, if $(a, 99) = 3$, then $(a^m, 99) = 9$ for $m > 1$, so the answer is $\boxed{\mathbf{No}}$, there is no universal m (although interestingly, when n is squarefree there are no such problems).

Problem 2. (*20 pts: 5+5+5+5*)
(a) Calculate the greatest common divisor of 123 and 426.

Solution. With an eye towards the rest of the problem, it's best to use the Euclidean algorithm in full detail. In the left column we use the division algorithm, and in the right column we write each remainder in terms of 123 and 426.

$$\begin{array}{c|c} 426 = 3 \cdot 123 + 57 & 57 = 426 - 3 \cdot 123 \\ 123 = 2 \cdot 57 + 9 & 9 = -2 \cdot 426 + 7 \cdot 123 \\ 57 = 6 \cdot 9 + \boxed{\mathbf{3}} & 3 = 13 \cdot 426 - 45 \cdot 123 \\ 9 = 3 \cdot 3 + 0 & \end{array}$$

Thus $(123, 426) = \boxed{\mathbf{3}}$.

(b) Are there solutions to the equation

$$123x + 426y = 8?$$

If so, characterize them all.

Solution. The equation $ax + by = c$ has a solution if and only if $(a, b) \mid c$. In this case, we have $3 \nmid 8$, so there are $\boxed{\textbf{No solutions}}$.

(c) Are there solutions to the congruence

$$123x \equiv 12 \pmod{426}?$$

If so, characterize them all.

Solution. The equation $ax \equiv c \pmod{b}$ has solutions if and only if $(a, b) \mid c$. In the case that there are solutions, they may be found using the Euclidean algorithm.

Here we have $3 \mid 12$, so there are solutions, and we must begin by dividing the entire equation by the greatest common divisor. Thus we need to solve $41x \equiv 4 \pmod{142}$. From the Euclidean algorithm, we know that

$$13 \cdot 426 - 45 \cdot 123 = 3,$$

and dividing by 3 gives

$$13 \cdot 142 - 45 \cdot 41 = 1.$$

In other words, $-45 \cdot 41 \equiv 1 \pmod{142}$, so $\overline{41} \equiv -45 \equiv 97 \pmod{142}$. Thus

$$\begin{aligned} & 41x \equiv 4 \pmod{142} \\ \Rightarrow \quad & x \equiv \overline{41} \cdot 4 \equiv 388 \pmod{142} \\ \Rightarrow \quad & \boxed{\boldsymbol{x \equiv 104 \pmod{142}}} . \end{aligned}$$

(d) Find the least common multiple of 123 and 426 (you may leave the answer as a product).

Solution. For any integers a, b, we have $(a,b)[a,b] = ab$, so $[a,b] = ab\ (a,b)$. In this case,

$$[123, 426] = \frac{123 \cdot 426}{3} = 41 \cdot 426 = 17466.$$

Problem 3. (*10 pts*) Show that $(n-1)! \equiv 0 \pmod{n}$ for composite $n > 4$.
Hint: Be sure that your proof works for the case $n = p^2$ where p is prime.

Solution. Suppose that there is some proper divisor $d \mid n$ such that $d \neq \frac{n}{d}$. Then $1 < d < n$ and $1 < \frac{n}{d} < n$, so $d \cdot \frac{n}{d} = n \mid (n-1)!$

The preceding argument only fails if $n = p^2$ for a prime p, and by assumption this case only arises for $p \geq 3$. Then both $1 < p < n$ and $1 < 2p < n$, so $p \cdot 2p \mid (n-1)!$

(Bonus) (*5 pts*) Describe precisely all n such that $(n-1)! \not\equiv 0 \pmod{n^2}$.

Solution. The condition $(n-1)! \not\equiv 0 \pmod{n^2}$ is satisfied if and only if $\boxed{\boldsymbol{n = p} \text{ or } \boldsymbol{2p}}$ for a prime p, or $\boxed{\boldsymbol{n = 4, 8, 9}}$.

Problem 4. (*20 pts: 15+5*)
(a) Solve the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

Solution. The first two congruences combine immediately to give $x \equiv 2 \pmod{30}$. Plugging this into the third congruence implies

$$\begin{aligned} x = 2 + 30u &\equiv 3 \pmod{7} \\ \Rightarrow 2u &\equiv 1 \pmod{7} \\ \Rightarrow u &\equiv 4 \pmod{7}. \end{aligned}$$

Thus $\boxed{\boldsymbol{x = 2 + 30(4 + 7v) \equiv 122 \pmod{210}}}$.

(b) Determine whether there are any solutions to the system

$$\begin{aligned} x &\equiv 2 \pmod{10} \\ x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{14}. \end{aligned}$$

Solution. Break each congruence into prime factors and check for consistency:

$$\begin{aligned} x &\equiv 0 \pmod{2}, & x &\equiv 2 \pmod{5} \\ x &\equiv 0 \pmod{2}, & x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{2}, & x &\equiv 3 \pmod{7}. \end{aligned}$$

There is a contradiction modulo 2, so there are $\boxed{\textbf{No solutions}}$.

Problem 5. (*15 pts: 10+5*)
(a) Observe that the function $f(n) = n$ is totally multiplicative. Is $F(n) := \sum_{d|n} d$ totally multiplicative? Is $F(n)$ multiplicative?

Solution. The theory of multiplicative functions implies that $\boxed{F \textbf{ is multiplicative}}$. However, $F(p^2) = 1+p+p^2 \neq (1+p)^2 = F(p)\cdot F(p)$, so $\boxed{F \textbf{ is not totally multiplicative}}$.

(b) Prove that if f is totally multiplicative, then $\prod_{d|n} f(d) = f(n)^{d(n)/2}$, where $d(n)$ is the number of divisors of n.

Solution. Denote the desired product by $F(n)$. Squaring gives

$$\begin{aligned} F(n)^2 &= \prod_{d|n} f(d) \prod_{d|n} f(d) = \prod_{d|n} f(d) \prod_{d|n} f\left(\frac{n}{d}\right) = \prod_{d|n} f(d) f\left(\frac{n}{d}\right) \\ &= \prod_{d|n} f(n) = f(n)^{d(n)}. \end{aligned}$$

Taking the square root gives the claimed formula (strictly speaking, the formula in the problem statement should read $\pm f(n)^{d(n)/2}$ if n is square).

Problem 6. (*15 pts: 10+5*)
(a) Use the repeated squaring method to efficiently calculate $3^{91} \pmod{91}$.

Solution. First, write $91 = 1011011$ in binary. Now use these digits to calculate

$$\begin{aligned} 3^2 &= (3^{\mathbf{1}})^2 3^{\mathbf{0}} \equiv 9 \pmod{91} \\ 3^5 &= ((3^{\mathbf{1}})^2 3^{\mathbf{0}^2} 3^{\mathbf{1}} \equiv 61 \pmod{91} \\ 3^{11} &= (((3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}})^2 3^{\mathbf{1}} \equiv 61 \pmod{91} \\ 3^{22} &= ((((3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}})^2 3^{\mathbf{1}})^2 3^{\mathbf{0}} \equiv 81 \pmod{91} \\ 3^{45} &= (((((3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}})^2 3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}} \equiv 27 \pmod{91} \\ 3^{91} &= ((((((3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}})^2 3^{\mathbf{1}})^2 3^{\mathbf{0}})^2 3^{\mathbf{1}})^2 3^{\mathbf{1}} \equiv \boxed{\mathbf{3 \pmod{91}}}. \end{aligned}$$

(b) Is 91 a probable prime for the base 3? Is 91 a strong probable prime for the base 3?

Solution. Since $3^{91} \equiv 3 \pmod{91}$, $\boxed{\textbf{Yes}}$, 91 is a probable prime for the base 3.

However, since $3^{45} \equiv 27 \not\equiv \pm 1 \pmod{91}$, $\boxed{\textbf{No}}$, 91 is not a strong probable prime for the base 3.