

18.781 Exam 1 Solutions - Fall 2009

Thursday, Oct. 8

Problem 1. (*Short answer; 4 pts each*) Unless asked otherwise, you are not required to show detailed work for these questions, but you should give a brief explanation (“yes” and “no” are not acceptable answers).

(a) Evaluate $\phi(48)$ and $\phi(57)$.

$$\phi(48) = \phi(16) \cdot \phi(3) = 8 \cdot 2 = 16 \quad \phi(57) = \phi(19) \cdot \phi(3) = 18 \cdot 2 = 36$$

(b) If $7a - 34b = -5$, what can you conclude about the greatest common divisor (a, b) ?

It must divide 5 (i.e. it must be 5 or 1).

(c) We know that $\phi(n) = \sum_{d|n} \mu(n/d)d$. Evaluate this sum for $n = 1848$ by writing out all the non-zero terms.

$$\begin{aligned} \phi(1848) = & 1848 - 1848/2 - 1848/3 - 1848/7 - 1848/11 + 1848/6 + 1848/14 + 1848/21 + 1848/22 \\ & + 1848/33 + 1848/77 - 1848/42 - 1848/66 - 1848/154 - 1848/231 + 1848/462 \end{aligned}$$

(d) Is $37^{37} + 73^{73}$ a multiple of 7?

Firstly, we have $37^{37} + 73^{73} \equiv 2^{37} + 3^{73} \pmod{7}$. By Fermat's theorem, $2^3 \equiv 2 \pmod{7}$ and $3^3 \equiv 3 \pmod{7}$. Thus we have $37^{37} + 73^{73} \equiv 5 \pmod{7}$. So **no**.

(e) Is there an integer $m > 1$ that guarantees that $a^m \equiv a \pmod{143}$ for any a satisfying $(a, 143) = 1$? Is there a value of m that works for all integers a ?

Yes. By Fermat, $a^{121} \equiv a \pmod{11}$ and $a^{121} \equiv a \pmod{13}$ for any a , so by CRT, this works for all $a \pmod{143}$.

Problem 2. (20 pts: 5+5+5+5)

(a) Calculate the greatest common divisor of 172 and 308.

$$308 = 172 + 136$$

$$136 = 308 - 172$$

$$172 = 136 + 36$$

$$36 = 2 \cdot 172 - 308$$

$$136 = 3 \cdot 36 + 28$$

$$28 = 4 \cdot 308 - 7 \cdot 172$$

$$36 = 28 + 8$$

$$8 = 9 \cdot 172 - 5 \cdot 308$$

$$28 = 3 \cdot 8 + 4$$

$$4 = 19 \cdot 308 - 34 \cdot 172$$

Since $4|8$, the $\gcd(308, 172) = 4$.

(b) Are there solutions to the equation

$$172x + 308y = 8?$$

If so, characterize them all.

Yes, there are solutions since $(172, 308)|8$. One is $x = 9$ and $y = -5$. All other solutions are of the form $x = 9 + 77 \cdot a$ and $y = -5 - 43 \cdot a$.

(c) Are there solutions to the congruence

$$308x \equiv 12 \pmod{172}?$$

If so, characterize them all.

Yes, there are solutions since $(172, 308)|12$. One is $x = 57$ (since $57 \cdot 308 - 102 \cdot 172 = 12$). All other solutions are of the form $x = 57 + 43 \cdot a$ since $43 = 172/(172, 308)$.

Problem 3. (15 pts: 5+5+5)

For any prime $p > 3$, and any integer a :

- a) Prove that $a^2 + a + 1 \equiv 0 \pmod{p}$ if and only if a has order 3 \pmod{p} .

First, if a has order 3, then $a^3 - 1 = (a - 1)(a^2 + a + 1) \equiv 0 \pmod{p}$. Since a has order 3, $a - 1 \not\equiv 0 \pmod{p}$, so we must have $a^2 + a + 1 \equiv 0 \pmod{p}$.

If $a^2 + a + 1 \equiv 0 \pmod{p}$, then by the factorization above, $a^3 \equiv 1 \pmod{p}$. Thus, we need only prove that a does not have order 1, that is, that $a \not\equiv 1 \pmod{p}$. Since $p > 3$, we have $1^2 + 1 + 1 \not\equiv 0 \pmod{p}$, so a must have order exactly 3.

- b) Prove that a has order 3 \pmod{p} if and only if $a + 1$ has order 6 \pmod{p} .

If a has order 3, then $(a + 1)^3 = a^3 + 3a^2 + 3a + 1 = (a + 2)(a^2 + a + 1) - 1 \equiv -1 \pmod{p}$. Thus $(a + 1)^6 \equiv 1 \pmod{p}$. Thus $a + 1$ has order 6 or 2, and it cannot have order 2, since then we would have $a \equiv -2 \pmod{p}$, and $(-2)^3 - 1 = -9$, so -2 does not have order 3 modulo any $p > 3$.

if $a + 1$ has order 6, then $(a + 1)^3 \equiv -1 \pmod{p}$. So, by the factorization above $(a + 2)(a^2 + a + 1) \equiv 0 \pmod{p}$. The first term is not zero, because $a + 1 \not\equiv -1$, so $a^2 + a + 1 \equiv 0 \pmod{p}$ so a has order 3.

if you did part c) first: $a^2 + a + 1 \equiv 0 \pmod{p}$ if and only if $(a + 1)^2 - (a + 1) + 1 \equiv 0 \pmod{p}$.

- c) Prove that $a^2 - a + 1 \equiv 0 \pmod{p}$ if and only if a has order 6 \pmod{p} .

First, if a has order 6, then $a^3 + 1 = (a + 1)(a^2 - a + 1) \equiv 0 \pmod{p}$. Since a has order 6, $a + 1 \not\equiv 0 \pmod{p}$, so we must have $a^2 - a + 1 \equiv 0 \pmod{p}$.

If $a^2 - a + 1 \equiv 0 \pmod{p}$, then by the factorization above, $a^3 \equiv -1 \pmod{p}$. Thus, we need only prove that a does not have order 2, that is, that $a \not\equiv -1 \pmod{p}$. Since $p > 3$, we have $(-1)^2 - (-1) + 1 = 3 \not\equiv 0 \pmod{p}$, so a must have order exactly 6.

if you did part b) first: We have $a^2 - a + 1 \equiv (a - 1)^2 + (a - 1) + 1$ so a satisfies this polynomial if and only if $a - 1$ has order 3, by part (a). By part (b), this implies that a has order 6.

Problem 4. (15 pts: 10+5)

(a) Solve the system of congruences

$$\begin{aligned}x &\equiv 4 \pmod{7} \\x &\equiv 5 \pmod{8} \\x &\equiv 2 \pmod{9}.\end{aligned}$$

We have

$$7 \cdot 8 = 56 \equiv 2 \pmod{9} \quad 56 \equiv 0 \pmod{8} \quad 56 \equiv 0 \pmod{7}$$

$$7 \cdot 9 = 63 \equiv 0 \pmod{9} \quad 63 \equiv -1 \pmod{8} \quad 63 \equiv 0 \pmod{7}$$

$$8 \cdot 9 = 72 \equiv 0 \pmod{9} \quad 72 \equiv 0 \pmod{8} \quad 2 \equiv 2 \pmod{7}$$

Thus, $x = 56 - 5 \cdot 63 + 2 \cdot 72 = -115$.

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

$$\begin{aligned}x &\equiv 4 \pmod{14} \\x &\equiv 5 \pmod{16} \\x &\equiv 2 \pmod{18}.\end{aligned}$$

There are none, since any solution to the second equation would be odd, and any solution to the first would be even

Problem 5. (15 pts: 10+5)

(a) Observe that the function $f(n) = n^3$ is totally multiplicative. Is $F(n) := \sum_{d|n} d^3$ totally multiplicative? Is $F(n)$ multiplicative?

$F(n)$ is not totally multiplicative: $F(2) = 9$ and $F(4) = 73 \neq 9^2$. However, $F(n)$ is multiplicative, since it is obtained by summing a multiplicative function over divisors.

(b) Is there a function $g(n)$ such that $\log n = \sum_{d|n} g(d)$? If so, describe it as explicitly as possible.

By Möbius inversion, there must be such a function, given by

$$g(n) = \sum_{d|n} \mu(n/d) \log d.$$

If the primes that divide n are p_1, \dots, p_m , and $m > 1$ then we can rewrite this sum as

$$\begin{aligned} g(n) &= \log n - \sum_{i=1}^m \log(n/p_i) + \sum_{1 < i < j < n} \log(n/p_i p_j) - \sum_{1 < i < j < k < n} \log(n/p_i p_j p_k) \cdots \\ &= \log n - \sum_{i=1}^m (\log(n) - \log(p_i)) + \sum_{1 < i < j < n} (\log(n) - \log(p_i) - \log(p_j)) - \cdots = 0 \end{aligned}$$

Thus, $g(n)$ is only non-zero for prime powers, and $g(p^m) = \log p^m - \log p^{m-1} = \log p$.

Problem 6. (15 pts: 10+5)

(a) Use the repeated squaring method to efficiently calculate $12^{65} \pmod{65}$.

$$\begin{array}{lll} 12^1 \equiv 12 \pmod{65} & 12^2 \equiv 14 \pmod{65} & 12^4 \equiv 1 \pmod{65} \\ 12^8 \equiv 1 \pmod{65} & 12^{16} \equiv 1 \pmod{65} & 12^{32} \equiv 1 \pmod{65} \\ & 12^{64} \equiv 1 \pmod{65} & \end{array}$$

So,

$$12^{65} \equiv 12^{64} \cdot 12 \equiv 12.$$

(b) Is 65 a probable prime for the base 3? Is 65 a strong probable prime for the base 3?

Yes, it is a probable prime.

To test for strong probable primality, note that $12^2 \equiv 14 \not\equiv -1 \pmod{65}$ and $12^4 \equiv 1 \pmod{65}$. So 65 is not a strong probable prime to the base 12.