MAS 4203 - FINAL EXAM - Summer 2015

Thursday, August 6

NAME: Sol 1

Instructions: All work should be written in a proper and coherent manner, and in a way that any student in the class can follow your work. Show all necessary working and reasoning. When giving proofs your reasoning should be clear. Only scientific or basic calculators are allowed.

There are two parts A & B. Part A has 7 questions. Do six complete questions. If you do 7 then the best 6 will be taken. Part B is a bonus question.

TOTAL POINTS: 60 (+ 3 bonus)

PART A

In this part there are 7 questions. Do 6 complete questions, otherwise the best 6 will be taken.

1. [5x2 = 10 pts]

(a) Complete the Definition: An arithmetic function f is multiplicative if $f(mn) = f(m)f(n)$ whenever m, n are positive relatively prime integers.

(b) Prove that if f is multiplicative then $f(1) = 0$ or 1.

Suppose f is multiplicative. $(1,1) = 1$ so

$f(1) = f(1 \cdot 1) = f(1)f(1)$ (since f is multiplicative)

$f(1)(f(1) - 1) = 0$.

So either $f(1) = 0$ or $f(1) = 1$.

(c) Complete the Theorem: Let f be an arithmetic function and for $n \in \mathbb{Z}$, $n > 0$ let

$$F(n) = \sum_{d \mid n} f(d).$$

If f is multiplicative then F is multiplicative.

(d) Prove that if f and g are multiplicative functions then $h(n) = f(n)\,g(n)$ is also multiplicative.

Suppose f, g are multiplicative & m, n are positive relatively prime integers. Then

$h(mn) = f(mn)\,g(mn) = f(m)f(n)\,g(m)\,g(n)$ (since f, g are mult.)

$= f(m)g(m)\,f(n)g(n) = h(m)\,h(n)$ & h is multiplicative.

(e) Define ρ be $\rho(1) = 1$ and $\rho(n) = 2^m$ where m is the number of distinct prime numbers in the prime factorization of n. Prove or disprove that ρ is completely multiplicative.

We show ρ is not completely multiplicative.

$\rho(2) = \rho(2^1) = 2$

$\rho(2 \cdot 3) = \rho(2 \cdot 3) = 2^2$

$\rho(2^2 \cdot 3^2) = 2^2$ So,

$\rho(6 \cdot 6) = 2^2 \neq 4 = \rho(6)\,\rho(6)$.

& ρ is not completely multiplicative.

2. [2+2+3+3 = 10 pts]

Definition: Let $n \in \mathbb{Z}$ with $n > 0$. If k is a positive integer then

$$\sigma_k(n) = \sum_{d|n} d^k$$

(a) Find $\sigma_3(12)$ and $\sigma_4(8)$.

$\sigma_3(4) = 1 + 2^3 + 4^3 = 1 + 8 + 8^2 = \frac{8^2-1}{8-1} = 73$

$\sigma_3(3) = 1 + 3^3 = 28$ since σ_3 is mult. (see (b))

so $\sigma_3(n) = \sigma_3(4)\sigma_3(3) = 28 \cdot 73 = 2044$.

$\sigma_4(8) = 1 + 2^4 + 4^4 + 8^4 = 1 + 16 + 16^2 + 16^3 = \frac{16^4-1}{16-1} = 4369$

(b) Prove that $\sigma_k(n)$ is multiplicative.

The function $f(n) = n^k$ is multiplicative since

$f(mn) = (mn)^k = m^k n^k = f(m)f(n)$ if $(m,n) = 1$.

so $\sigma_k(n) = \sum_{d|n} d^k = \sum_{d|n} f(d)$ is multiplicative

by Thm 3.1.

(c) Find a formula for $\sigma_k(p^a)$ if p is prime and a is a positive integer.

$$\sigma_k(p^a) = \sum_{d|p^a} d^k = 1 + p^k + (p^2)^k + \cdots + (p^a)^k$$

$$= 1 + p^k + (p^k)^2 + \cdots + (p^k)^a$$

$$= \frac{(p^k)^{a+1} - 1}{p^k - 1}$$

(d) Let $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ be a prime factorization where each $a_i > 0$. Find a formula for $\sigma_k(n)$ using (b) & (c).

$$\sigma_k(n) = \sigma_k(p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m})$$
$$= \sigma_k(p_1^{a_1})\,\sigma_k(p_2^{a_2}) \cdots \sigma_k(p_m^{a_m}) \quad \text{(since } \sigma_k \text{ is multiplicative)}$$
$$= \left(\frac{(p_1^k)^{a_1+1} - 1}{p_1^k - 1}\right)\left(\frac{(p_2^k)^{a_2+1} - 1}{p_2^k - 1}\right) \cdots \left(\frac{(p_m^k)^{a_m+1} - 1}{p_m^k - 1}\right) \quad \text{by (c).}$$

3. [2+3+2+3 = 10 pts]

(i) Complete Theorem: Let $n \in \mathbb{Z}$, $n > 1$. Then

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

where p = prime.

(ii) Prove or disprove that there are infinitely many integers n such that

$$\phi(n) = \frac{n}{3}.$$

We prove the result:

Let $n = 2^m \cdot 3$ for $m \geq 1$. Then by (i)

$$\phi(n) = n\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right) = n \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} = \frac{n}{3}.$$

So $\phi(n) = n/3$ for infinitely many n.

(iii) Complete Theorem: Let $n \in \mathbb{Z}$, $n > 0$. Then n is an even perfect number if and only if

$$n = 2^{p-1}(2^p - 1)$$

where $2^p - 1$ is a Mersenne prime.

(iv) Definition a positive integer n is super perfect if $\sigma(\sigma(n)) = 2n$.

Prove that if $2^p - 1$ is a Mersenne prime then 2^{p-1} is super perfect.

Suppose $2^p - 1$ is a Mersenne prime.

~~Then $\sigma(2^p-1) = 1 + (2^p-1)$ since 2^p-1 is prime.~~

$\sigma(2^{p-1}) = (2^p - 1)/(2-1) = 2^p - 1$

$\sigma(2^p - 1) = 1 + (2^{p-1}) = 2^p$ since (2^p-1) is prime

$\therefore \sigma(\sigma(2^{p-1})) = 2^p = 2 \cdot 2^{p-1}$ &

2^{p-1} is super perfect.

4. [2+2+2+4 = 10 pts]

(a) Complete the Definition: Let $n \in \mathbb{Z}$, with $n > 0$.

The Möbius function denoted $\mu(n)$ is

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ some prime } p \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ where } p_1, p_2, \ldots, p_k \text{ are distinct.} \end{cases}$$

(b) Complete the Theorem: Let $n \in \mathbb{Z}$ with $n > 0$.

Then

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$$

(c) Complete the Möbius Inversion Formula: Let f, g be arithmetic functions. Then

$$f(n) = \sum_{d|n} g(d) \quad \text{for all } n \geq 1,$$

if and only if

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \quad \text{for all } n \geq 1.$$

(d) Let $\tau(n)$ = number of positive divisors of n. Prove that

$$\tau(n) = \sum_{d|n} \mu(d)\, \tau\left(\frac{n}{d}\right).$$

$$\tau(n) = \sum_{d|n} 1.$$

Let $g(n) = 1$ for $n \geq 1$. Use by Möbius inversion

$$g(n) = 1 = \sum_{d|n} \mu(d)\, \tau\left(\frac{n}{d}\right),$$

$$1 = \sum_{d|n} \mu(d)\, \tau\left(\frac{n}{d}\right)$$

for all $n \geq 1$.

5. [2+2+4+2 = 10pts]

(a) Complete Euler's Criterion: Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(b) Complete Theorem: Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8, \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

(c) Do ONE part.

(i) Prove or disprove that there is a integer n such that n^2+2 is divisible by 2019.

(ii) Let p, q be primes with $p \equiv 3 \pmod 4$, and $q = 2p+1$. Prove that q divides $2^p - 1$.

(i) $2019 = 3 \cdot 673$. $n^2+2 \equiv 0 \pmod 3$ for $n \equiv 1 \pmod 3$.

$$\left(\frac{-2}{673}\right) = \left(\frac{-1}{673}\right)\left(\frac{2}{673}\right) = (+1)(+1) = +1.$$

since $673 = 84 \cdot 8 + 1$ & $673 \equiv 1 \pmod 4$ & $673 \equiv 1 \pmod 8$.

So -2 is a qr. mod 673, there is a $m_0 \in \mathbb{Z}$: $m_0^2 \equiv -2 \pmod{673}$.

By Chinese Remainder Thm we can solve $x \equiv 1 \pmod 3$, $x \equiv m_0 \pmod{673}$

Then $x^2 \equiv -2 \pmod 3$ & $x^2 \equiv -2 \pmod{673}$ & so $2019 = 3 \cdot 673 \mid x^2+2$.

The statement is true.

(ii) $p \equiv 3 \pmod 4$ so $p = 4k+3$ some $k \in \mathbb{Z}^+$.

& $q = 2p+1 = 2(4k+3)+1 = 8k+7 \equiv 7 \pmod 8$.

So $\left(\frac{2}{q}\right) = +1$. But by Euler $\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \pmod q$ & (p. 2)
so $1 \equiv 2^p \pmod q$ & hence
$q \mid (2^p - 1)$.

(d) Find a prime p for which $2^p - 1$ is composite. Show all reasoning.

$p = 11 \equiv 3 \pmod 4$ &
$q = 2p+1 = 23$ is prime. So by (c)
$23 \mid (2^{11} - 1)$ & $2^p - 1$ is composite when $p = 11$.

6. [4 + 6 = 10 pts]

(a) Complete the Law of Quadratic Reciprocity:
Let p, q be distinct odd primes.
Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

If p or $q \equiv 1 \pmod 4$ then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

If $p \equiv q \equiv 3 \pmod 4$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(b) Find the Legendre symbol $\left(\frac{501}{773}\right)$. Show all reasoning.

$\left(\frac{501}{773}\right) = \left(\frac{-272}{773}\right)$ since $501 \equiv -272 \pmod{773}$

$= \left(\frac{-1}{773}\right)\left(\frac{2^4}{773}\right)\left(\frac{17}{773}\right)$ since $-272 = -1 \cdot 2^4 \cdot 17$

$= (+1)(+1)\left(\frac{17}{773}\right)$ since $773 \equiv 1 \pmod 4$ & $2^4 = 4^2$.

$= \left(\frac{773}{17}\right)$ by LQR since $773 \equiv 1 \pmod 4$

$= \left(\frac{8}{17}\right)$ since $773 \equiv 8 \pmod{17}$

$= \left(\frac{2}{17}\right)^3$ since $8 = 2^3$

$= 1$ since $8 \equiv 1 \pmod{17}$.

See Athdal for other sch

7. [10 pts]

Do ONE part.

(a) Explain and describe the RSA encryption scheme and give a proof of the decoding procedure.

(b) State the a-test for primality and prove that p passes the a-test for all odd primes $p > a$ where a is any fixed integer $a > 1$.

See attached

6(b) ALT. SOLN

$$\left(\frac{501}{773}\right) = \left(\frac{3}{773}\right)\left(\frac{167}{773}\right) \quad \text{since } 501 = 3 \cdot 167$$

$$= \left(\frac{773}{3}\right)\left(\frac{773}{167}\right) \quad \text{by LQR since } 773 \equiv 1 \pmod 4$$

$$= \left(\frac{2}{3}\right)\left(\frac{105}{167}\right) \quad \text{since } 773 \equiv 2 \pmod 3,\ 773 \equiv 105 \pmod{167}$$

$$= (-1)\left(\frac{3}{167}\right)\left(\frac{5}{167}\right)\left(\frac{7}{167}\right) \quad \text{since } 3 \equiv 3 \pmod 8 \text{ \& } 105 = 3 \cdot 5 \cdot 7.$$

$$= (-1)\left(-\left(\frac{167}{3}\right)\right)\left(\frac{167}{5}\right)\left(-\left(\frac{167}{7}\right)\right) \quad \text{by LQR}$$

since $3, 7, 167 \equiv 3 \pmod 4$ & $5 \equiv 1 \pmod 4$.

$$= -\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{6}{7}\right) \quad \text{since } 167 \equiv 2, 2, 6 \pmod{3, 5, 7 \text{ resp.}}$$

$$= (-1)(-1)(-1)\left(\frac{-1}{7}\right) \quad \text{since } 3, 5 \equiv 3, 5 \pmod 8,\ 6 \equiv -1 \pmod 7$$

$$= 0 - (-1) \quad \text{since } 7 \equiv 3 \pmod 4$$

$$= +1.$$

7(a)

+3 For description of RSA scheme

(a key)

Thus B has recovered

$$M = 1615140019110120050519$$

which easily translates to

JON SKATES

Theorem (Proof of The Decoding Procedure)

Suppose p and q are distinct primes.

$$n = pq,$$

Suppose the positive integer r satisfies $(r, (p-1)(q-1)) = 1$ and s is a positive integer such that

$$rs \equiv 1 \pmod{(p-1)(q-1)}$$

Let M be a positive integer. Suppose $M < n$ and

$$E \equiv M^r \pmod{n}$$

Then

$$E^s \equiv M \pmod{n}.$$

+7 PROOF: Suppose all the hypotheses hold.

Since p and q are distinct primes,

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Since $rs \equiv 1 \pmod{(p-1)(q-1)}$, there is a nonnegative integer d such that

$$rs = d(p-1)(q-1) + 1.$$

We consider 2 cases.

We must show that

$$E^s \equiv M^{rs} \equiv M \pmod{n}$$

Case 1. $(M, n) = 1$. Then $\phi(n) = (p-1)(q-1)$

By Euler's Theorem

$$M^{\phi(n)} = M^{(p-1)(q-1)} \equiv 1 \pmod{n}.$$

So

$$M^{rs} = M^{d(p-1)(q-1)+1} = \left(M^{(p-1)(q-1)}\right)^d M^1$$

$$\equiv 1^d \cdot M^1 \pmod{n}$$

$$\equiv M \pmod{n}$$

Case 2 $(M, n) > 1$. We may assume without loss of generality that $(M, p) = p$.

Then $M^{rs} \equiv M \pmod{p}$

since $p \mid M$ & $M \equiv 0 \pmod{p}$.

By Fermat's Little Theorem

$$M^{q-1} \equiv 1 \pmod{q}$$

since $(M, q) = 1$. Hence

$$M^{rs} = M^{d(p-1)(q-1)+1} = \left(M^{q-1}\right)^{d(p-1)} M^1$$

$$\equiv 1^{d(p-1)} M \pmod{q},$$

$$\equiv M \pmod{q}$$

This implies $M^{rs} \equiv M \pmod{n}$

since $n = pq$ & p, q are distinct primes.

In both cases

$$E \equiv M^{rs} \equiv M \pmod{n},$$

as required. □

Fermat's Little Theorem

Let p be prime, $a \in \mathbb{Z}$ and $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}$$

NOTE: The converse is not true.

For example $2^{340} \equiv 1 \pmod{341}$

but $341 = 11 \cdot 31$.

Lemma Let p be prime, and $a \in \mathbb{Z}$.

If $a^2 \equiv 1 \pmod{p}$ then

$$a \equiv \pm 1 \pmod{p}.$$

7(b)

The a-Test Let $a \in \mathbb{Z}$ with $a > 1$ be fixed.

Suppose N is a positive odd integer and $N > 1$.

Let $N - 1 = 2^r s$ where s is odd,

and assume $a < N$.

We say N passes the a-Test if

(1) $(a, N) = 1$,

(2) $a^{N-1} \equiv 1 \pmod{N}$

and (3) $a^s \equiv 1 \pmod{N}$

or $a^{(2^k s)} \equiv -1 \pmod{N}$

for some $0 \leq k \leq r-1$.

Theorem Let N be an odd prime, and suppose $a \in \mathbb{Z}$ and $1 < a < N$. Then N passes the a-Test.

Proof: Suppose N is prime, odd, $a \in \mathbb{Z}$ and $1 < a < N$.

(1) Since N is prime, $a < N$ we have $(a, N) = 1$.

(2) By Fermat's Little Theorem $a^{N-1} \equiv 1 \pmod{N}$, since N is prime a (since $1 < a < N$).

(3) Let $N - 1 = 2^r s$ where $r \geq 1$ and s is odd.

Let $K = \{k \in \mathbb{Z} : a^{2^k s} \equiv 1 \pmod{N} \ \& \ 0 \leq k \leq r\}$.

K is nonempty since $a^{N-1} \equiv 1 \pmod{N}$ & $r \in K$.
Hence K has a least element k_0.

Case 1 $k_0 = 0$. Then $a^{s} \equiv 1 \pmod{N}$

Case 2 $1 \leq k_0 \leq r$. We have

$$a^{(2^{k_0} s)} \equiv 1 \pmod{N},$$

$$\left(a^{2^{k-1} s}\right)^2 \equiv 1 \pmod{N}.$$

$$a^{(2^{k_0 - 1} s)} \equiv \pm 1 \pmod{N}$$ since N is prime.

$(2^{k_0-1}, s)$

$a \equiv -1 \pmod N$ since $0 < k_0 - 1 < k_0$

as k_0 is smallest element of K. In this case

$(2^{k_1}, s)$

$a \equiv -1 \pmod N$ where $0 < k_1 \leq r-1$.

Hence N passes the a-Test.

Example $N = 341 = 11 \cdot 31$. Show that 341 fails the 2-test.

$N - 1 = 340 = 2 \cdot 170 = 2^2 \cdot 85$.

Here $r = 2$ & $s = 85$. $N = 341$ passes the 2-Test if $2^s = 2^{85} = \pm 1 \pmod{341}$,

or $2^{2s} = (2^{85})^2 \equiv -1 \pmod{341}$,

since we know as 341, 341 is pseudoprime & $2^{340} \equiv 1 \pmod{341}$.

By Fermat's Little Theorem,

$2^{10} \equiv 1 \pmod{11}$.

$2^{85} = (2^{10})^8 \cdot 2^5 \equiv 2^5 \equiv 32 \pmod{11}$.

$2^5 = 32 \equiv 1 \pmod{31}$ &

$2^{85} = (2^5)^{17} \equiv 1 \pmod{31} \equiv 32 \pmod{31}$.

It follows that $2^{85} \equiv 32 \pmod{341}$ &

$2^{85} \not\equiv -1 \pmod{341}$.

$(2^{85})^2 \equiv (-1)^2 \equiv 1 \pmod{11}$,

$(2^{85})^2 \equiv (32)^{17} \equiv 1^2 \equiv 1 \pmod{31}$ &

$2^{2 \cdot 85} \equiv 1 \pmod{341}$ &

$2^{2s} \not\equiv -1 \pmod{341}$.

Hence 341 fails the 2-Test & must be composite.

PART B [3 bonus pts] (p. 11)

(a) This is _____

He was born in 1927 in _____

In 1962 he proved that 78557 is a Sierpinski number. A Sierpinski number is a number k such that $k \cdot 2^n + 1$ is _____ for _____.

(b) This is _____

He received his PhD from _____ in 1972. He is the inventor of one of the most important integer _____ methods, the quadratic sieve algorithm.

(c) This is _____

He is a professor at _____. In a talk at the Bloomington Illinois Number Theory Conference John Selfridge came to his rescue hollering out with saying "He use the principle of computer _____ a _____."