FINAL EXAM SPRING 2009

1\. (i) Suppose a, m, n are positive integers, $a>1$, $n>1$ and $m \mid n$.

There is a positive integer d such that

$$n = md$$

since $m \mid n$ & m, n are positive.

$x^d - 1 = (x-1)(x^{d-1} + x^{d-2} + \cdots + x + 1)$ for $x \in \mathbb{R}$.

Letting $x = a^m$ we have

$$a^n - 1 = (a^m)^d - 1 = (a^m - 1)(a^{m(d-1)} + a^{m(d-2)} + \cdots + a^m + 1)$$

& $a^m - 1 \mid a^n - 1$

since $a^{m(d-1)} + a^{m(d-2)} + \cdots + a^m + 1 \in \mathbb{Z}$.

(ii) Suppose a, n are positive integers, $a>1$ & $n>1$, and suppose $a^n - 1$ is prime.

$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a^1 + 1)$.

So $(a-1) \mid (a^n - 1)$ since $a^{n-1} + a^{n-2} + \cdots + a^1 + 1 \in \mathbb{Z}$

$1 \leq a - 1 < a^n - 1$ since $a>1$ & $n>1$.

Since $a^n - 1$ is prime this implies that $a - 1 = 1$ & $a = 2$.

Suppose by way of contradiction that n is composite so that $n = md$ for some integers m, d satisfying $1 < m, d < n$.

$a^m - 1 \mid a^n - 1$ by (i) since $m \mid n$.

But $a^m - 1 = 2^m - 1 > 2 - 1 = 1$

& $a^m - 1 < a^n - 1$ which contradicts $a^n - 1$ being prime. Hence $a^n - 1$ must be prime. $\square$

2(i)

Suppose $a = 6n+1$, $b = 6m+1$ where $m, n \in \mathbb{Z}$.
Then

$$ab = (6n+1)(6m+1) = 36mn + 6n + 6m + 1$$
$$= 6(6mn + n + m) + 1$$

which has the desired form since $6mn + n + m \in \mathbb{Z}$.

(ii) Suppose by way of contradiction that there are only finitely many primes of the form $6n+5$ (where n is an integer) say

$$p_0 = 5, \; p_1, p_2, \ldots, p_r.$$

Let

$$N = 6p_1p_2\cdots p_r + 5.$$

Then N is an integer > 5 & must have at least one prime divisor. Clearly $2 \nmid N$ & $3 \nmid N$ so any prime divisor of N has the form $6n+1$ or $6n+5$ (by division algorithm ~~also~~ any positive integer has the form $6n + c$ where $c = 0, 1, 2, 3, 4$ or 5 & $2 \mid 6n+c$ for $c = 0, 2, 4$ & $3 \mid 6n+c$ when $c = 3$).
N must have at least one prime divisor of the form $6n+5$ since if every prime divisor of N is of the form $6n+1$ then N would be of the form $6n+1$ (by (i)), which contradicts the fact that N is clearly of the form $6n+5$.
Hence N must have at least one prime divisor p which is of the form $6n+5$, & $p = p_j$ for some $0 \le j \le r$.
<u>CASE (1)</u> $j = 0$ & $p = 5$. Then $5 \mid N$ & so

$$5 \mid N - 5 = 2 \cdot 3 \cdot p_1 \cdot p_2 \cdots p_r$$

and $5 = 2, 3, p_1, \ldots,$ or p_r by Euclid's Lemma which is impossible.

<u>Case 2</u> $1 \le j \le r$ & $p = p_j$.

So $p \mid 6 \cdot p_1 p_2 \cdots p_r$ &

$p \mid (N - 6 \cdot p_1 p_2 \cdots p_r) = 5$.

So $p = 5$ which is impossible since $p_j = p > 5$.

We have a contradiction in all cases & therefore there must be infinitely many primes of the form $6n+5$ (where $n \in \mathbb{Z}$).

3.

(i) We write $a \equiv b \pmod m$ when $m \mid (a-b)$.

(ii) Suppose $a, b, c, d, m \in \mathbb{Z}$ & $m > 0$.

Suppose $a \equiv b \pmod m$ & $c \equiv d \pmod m$.

Then $m \mid (a-b)$ & $m \mid (c-d)$.

Therefore

$$m \mid c(a-b) + b(c-d) \qquad (\text{since } c, b \in \mathbb{Z}).$$

But $c(a-b) + b(c-d) = ac - bd$ &

$m \mid ac - bd$ &

therefore $ac \equiv bd \pmod m$.

(iii) Suppose $a, b \in \mathbb{Z}$ & p is prime.

Suppose $a^2 \equiv b^2 \pmod p$.

Then $p \mid (a^2 - b^2) = (a-b)(a+b)$.

Therefore $p \mid (a-b)$ or $p \mid (a+b)$ by Euclid's Lemma since p is prime.

Thus either $a \equiv b \pmod p$ or $a \equiv -b \pmod p$.

(iv) If p is not prime (iii) is not necessarily true.

For example, $3^2 \equiv 1^2 \pmod 8$ since $8 \mid (3^2 - 1^2) = 8$.

But $3 \not\equiv 1 \pmod 8$ & $3 \equiv -1 \pmod 8$

since $8 \nmid 2$ & $8 \nmid 4$.

4(i)

<u>Fermat's Little Theorem</u> Suppose $a \in \mathbb{Z}$, p is prime & $p \nmid a$. Then

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

(ii) A positive integer n is <u>pseudoprime</u> if n is composite and

$$2^{n-1} \equiv 1 \pmod{n}.$$

(iii) Let $n = 645 = (3)(5)(43)$. Then clearly n is composite. To show that that

$$2^{n} \equiv 2 \pmod{n}$$

it suffices to show that

(*) $$2^{n} \equiv 1 \pmod{m} \text{ ie } 2^{645} \equiv 2 \pmod{m}$$

for $m = 3, 5$ and 43 since $3, 5, 43$ are pairwise relatively prime.

$$2^2 = 4 \equiv 1 \pmod{3}, \; \&$$

$$2^{644} = (2^2)^{322} \equiv 1^{322} \equiv 1 \pmod{3} \; \&$$

$$2^{645} = 2^{644} \cdot 2^1 \equiv 1 \cdot 2 \equiv 2 \pmod{3} \; \&$$

(*) holds for $m = 2$.

$$2^4 = 16 \equiv 1 \pmod{5}.$$

$$2^{645} = (2^4)^{161} \cdot 2^1 \equiv 1 \cdot 2 \equiv 2 \pmod{5} \; \&$$

(*) holds for $m = 5$.

By Fermat's Little Theorem, $2^{42} \equiv 1 \pmod{43}$ since 43 is an odd prime.

$$645 = 630 + 15 = 15 \cdot 42 + 15 \; \&$$

$$2^{645} = (2^{42})^{15} \cdot 2^{15} \equiv 2^{15} \pmod{43}.$$

$$2^5 = 32$$
$$2^6 = 64 \equiv 21 \pmod{43},$$
$$2^7 \equiv 42 \equiv -1 \pmod{43},$$
$$2^{14} \equiv (-1)^2 \equiv 1 \pmod{43},$$
$$\& \quad 2^{15} \equiv 2 \pmod{43}.$$

Therefore, $2^{645} \equiv 2 \pmod{43}$ & $(*)$ holds for $m = 43$.
Hence $(*)$ holds for $m = 3, 5$ & 43 & 645 is a pseudo prime.

(iv) Suppose p & q are distinct primes & $a \in \mathbb{Z}$.
Then

$$a^p \equiv a \pmod{p} \quad \text{(by Corollary to Fermat's Little Thm.)}$$

and

$$a^{pq} = (a^p)^q \equiv a^q \pmod{p}.$$

Therefore,

$$a^{pq} + a \equiv a^q + a^p \equiv a^p + a^q \pmod{p}.$$

Similarly,

$$a^q \equiv a \pmod{q},$$
$$a^{pq} = (a^q)^p \equiv a^p \pmod{q} \;\&$$
$$a^{pq} + a \equiv a^p + a^q \pmod{q}.$$

Hence

$$a^{pq} + a \equiv a^p + a^q \pmod{m}$$

for $m = p$ & $m = q$. Since p & q are distinct primes the result follows.

5.

(i) An arithmetic function f is <u>multiplicative</u> if
$$f(mn) = f(m)\,f(n)$$
whenever ~~...~~ m & n are relatively prime positive integers.

(ii) Suppose f is multiplicative.
$(1,1) = 1$ & so
$$f(1\cdot 1) = f(1)\,f(1),$$
$$f(1)(f(1) - 1) = 0.$$
Thus either $f(1) = 0$ or $f(1) = 1$.

(iii) Suppose f, g are multiplicative & m, n are positive relatively prime integers.
$$\begin{aligned} h(mn) &= f(mn)\,g(mn) \\ &= f(m)f(n)\,g(m)\,g(n) \quad \text{(since } f, g \text{ are multiplicative)} \\ &= (f(m)\,g(m))(f(n)\,g(n)) \\ &= h(m)\,h(n). \end{aligned}$$
Hence h is multiplicative.

(iv)
$$\mu(n) := \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ (product of distinct primes)} \\ 0 & \text{if } p^2 \mid n \text{ some prime } p. \end{cases}$$

Theorem

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

(v) Suppose f is multiplicative, $f(1) = 1$ & $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is a prime factorization of n.

Then

$\mu(n) f(n)$ is multiplicative by (iii) since μ & f are multiplicative. Therefore,

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

is multiplicative by theorem 3.1.

$$F(p_j^{a_j}) = \sum_{d \mid p_j^{a_j}} \mu(d)\, f(d)$$

$$= \mu(1) f(1) + \mu(p_j) f(p_j) + \mu(p_j^2) f(p_j^2) + \cdots + \mu(p_j^{a_j}) f(p_j^{a_j})$$

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

Hence

$$F(n) = \sum_{d \mid n} \mu(d) f(d) = F(p_1^{a_1}) F(p_2^{a_2}) \cdots F(p_m^{a_m})$$

(since F is multiplicative)

$$= (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_m))$$

$$= \prod_{i=1}^{m} (1 - f(p_i)).$$

6 (p 8)

(i) $\phi(n)$ = the number of integers m where $1 \leq m \leq n$ & $(m,n)=1$.

$\nu(n)$ = The number of positive divisors of n.

$\sigma(n)$ = The sum of the positive divisors of n.

(ii) $\nu(n)$ is multiplicative by Theorem 3.1 since

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

& $f(n)=1$ is multiplicative.

$\sigma(n)$ is multiplicative by Theorem 3.1 since

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} g(d)$$

& $g(n)=n$ is multiplicative.

(iii) Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ is a prime factorization of $n>1$.

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_m^{a_m} - p_m^{a_m-1})$$
$$= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

$$\nu(n) = (1+a_1)(1+a_2) \cdots (1+a_m) = \prod_{i=1}^{m} (1+a_i)$$

$$\sigma(n) = \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{a_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_m^{a_m+1}-1}{p_m-1}\right)$$
$$= \prod_{i=1}^{m} \left(\frac{p_i^{a_i+1}-1}{p_i-1}\right)$$

$\nu(1) = 1$.

If $n = p_1^{a_1} \cdots p_m^{a_m} > 1$ (prime factorization) then
$\nu(n) = (1+a_1)(1+a_2)\cdots(1+a_m)$,
and $\nu(n)$ is odd iff $1+a_i$ is odd for all $1 \le i \le m$
ie a_i is even for all $1 \le i \le m$
which is equivalent to n being a perfect square.

[NOTE: If $n = p_1^{2b_1} p_2^{2b_2} \cdots p_m^{2b_m}$ where each $b_j > 0$ (integer)
then $n = (p_1^{b_1} \cdots p_m^{b_m})^2$ is a perfect square.
Conversely if
$n = m^2$ where m is a positive integer.
then $m = p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m}$ be a prime factorization &
$n = p_1^{2b_1} p_2^{2b_2} \cdots p_m^{2b_m}$.]

7.

(i) Suppose $a, m \in \mathbb{Z}$ with $m > 0$.
a is a quadratic residue modulo m if
$(a, m) = 1$ &
$x^2 \equiv a \pmod{m}$
for some $x \in \mathbb{Z}$.

(ii) Let $p = 17$. Then $\frac{p-1}{2} = 8$.

x	$x^2 \pmod{17}$
± 1	1
± 2	4
± 3	9
± 4	16
± 5	8
± 6	2
± 7	15
± 8	13

The quadratic residues mod 17 are 1, 2, 4, 8, 9, 13, 15, 16

(iii) Suppose p is an odd prime, $a \in \mathbb{Z}$ & $p \nmid a$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

~~(iv) Let p & q be~~

PROPERTIES Suppose p is an odd prime, $a, b \in \mathbb{Z}$ & $p \nmid a$ & $p \nmid b$. Then

(a) $\left(\frac{a^2}{p}\right) = 1$

(b) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iv) The Law of Quadratic Reciprocity

Suppose p & q are distinct odd primes.

Then

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

(v) $425 = 17 \cdot 25$

$\left(\frac{425}{149}\right) = \left(\frac{17}{149}\right)\left(\frac{25}{149}\right) = \left(\frac{17}{149}\right)$ since $25 = 5^2$.

$\left(\frac{17}{149}\right) = \left(\frac{149}{17}\right)$ (by the Law of Quadratic Reciprocity since $17 \equiv 1 \pmod{4}$)

$= \left(\frac{13}{17}\right)$ (since $149 = (17)(8) + 13$ & $149 \equiv 13 \pmod{17}$)

$= 1$ (by (ii)).