UNIVERSITY OF MANITOBA

DATE: March 10, 2010

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

MIDTERM II
PAGE: 1 of 5
TIME: 50 minutes
EXAMINER: M. Davidson

---

[15] 1. (a) Given the prime factorization of $n = 45\,864$ is $2^3 \cdot 3^2 \cdot 7^2 \cdot 13$, find $d(45\,864)$, $\sigma(45\,864)$ and $\phi(45\,864)$.

$d(45864) = 4 \cdot 3 \cdot 3 \cdot 2 = 72$

$\sigma(45864) = (1+2+4+8)(1+3+9)(1+7+49)(1+13)$

$= (2^4-1)\left(\frac{3^3-1}{2}\right)\left(\frac{7^3-1}{6}\right)(1+13) = 15 \cdot 13 \cdot 57 \cdot 14$

$= 155\,610$

$\phi(45864) = 2^2(2-1) \cdot 3(3-1) \cdot 7(7-1)(13-1)$

$= 4 \cdot 3 \cdot 2 \cdot 7 \cdot 6 \cdot 12 = 12096$

(b) If p and q are distinct primes, what is $d(p^2q)$, $\sigma(p^2q)$ and $\phi(p^2q)$?

$d(p^2q) = 3 \cdot 2 = 6$

$\sigma(p^2q) = (1+p+p^2)(1+q) = \left(\frac{p^3-1}{p-1}\right)(1+q)$

$\phi(p^2q) = p(p-1)(q-1)$

(c) Prove that if n is odd then $\phi(2n) = \phi(n)$ and if n is even then $\phi(2n) = 2\phi(n)$. [Hint: recall that if n is even then it can be express as $n = 2^e m$ where $e \geq 1$ and m is odd.]

If n is odd then $(2, n) = 1$

Since ϕ is multiplicative

$\phi(2n) = \phi(2)\phi(n) = (2-1)\phi(n) = \phi(n)$

If n is even then $n = 2^e m$ where $e \geq 1$ and m is odd

So $\phi(2n) = \phi(2^{e+1} m)$ since $(2^{e+1}, m) = 1$

$= \phi(2^{e+1})\phi(m)$

$= 2^e(2-1)\phi(m) = 2^e\phi(m)$

and $\phi(n) = \phi(2^e m) = 2^{e-1}(2-1)\phi(m) = 2^{e-1}\phi(m)$

So $\phi(2n) = 2\phi(n)$

---

[10] 2. Find the least residue of $x \pmod m$ for the following. State any theorem that you use.

(a) $x = 107^{2163}$ and $m = 433$ [Note: 433 is prime]

Using Fermat's Theorem: $107^{432} \equiv 1 \mod 433$

So $x = 107^{2163} \equiv (107^{432})^5 \cdot 107^3 \mod 433$

$\equiv 107^3 \mod 433$

$\equiv 1\,225\,043 \mod 433$

$\equiv 86 \mod 433$

(b) $x = 107^{2163}$ and $m = 432$ [Note: 432 is obviously not prime]

Using Euler's Theorem: $432 = 2^4 \cdot 3^3$ $\quad \phi(432) = 2^3 3^2 (3-1) = 144$

So $107^{144} \equiv 1 \mod 432$

$107^{2163} \equiv (107^{144})^{15} 107^3 \mod 432$

$\equiv 1225043 \mod 432$

$\equiv 323 \mod 432$

(c) $x = (432)(431)\cdots(44)(43)(41)(40)\cdots(3)(2)(1)$ and $m = 433$
[Note: 433 is still prime. Here, x is the product of all numbers less than or equal to 432 EXCEPT 42.]

Wilsons Theorem: $432! \equiv -1 \mod 433$

So $42x \equiv 432! \equiv -1 \mod 433$

$433 = 42(10) + 13$
$42 = 13(3) + 3$
$13 = 3(4) + 1$

$1 = 13 + 3(-4)$
$= 13 + [42 + 13(-3)](-4)$
$= 42(-4) + 13(13)$
$= 42(-4) + [433 + 42(-10)](13)$
$= 433(13) + 42(-134)$

$(-134)42x \equiv (-134)(-1) \mod 433$

$x \equiv 134 \mod 433$

---

[8] 3. (a) Define what if means for a number n to be perfect.

A number is perfect if

$\sigma(n) - n = n$

(b) Define what if means for a number n to be abundant.

A number is abundant if

$\sigma(n) - n > n$

(c) If n is an even perfect number, what is known about the prime factorization of n?

If n is an even perfect number then

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

where $2^p - 1$ (and hence p) is prime.

(d) Show that if n is an even perfect number then $5n$ is abundant.

If n is an even perfect number then

$n = 2^{p-1}(2^p - 1)$. Since $2^p - 1$ is prime, $5 \nmid 2^p - 1$

Hence $(n, 5) = 1$

So $\sigma(5n) = \sigma(5)\sigma(n)$

$= (5+1)(2n)$

$= 12n$

$12n - 5n = 7n > 5n$

So $5n$ is abundant.

---

[10] 4. (a) Define amicable and show that if m and n are amicable then $\sigma(m) = \sigma(n)$.

The numbers m & n are amicable

if $\sigma(m) - m = n$ and $\sigma(n) - n = m$.

$\sigma(m) - m = n \Rightarrow \sigma(m) = m + n$

$\sigma(n) - n = m \Rightarrow \sigma(n) = m + n$

So $\sigma(m) = \sigma(n)$

(b) Show that 6 232 and 6 368 are an amicable pair.
[Hint: 199 is prime and 779 is divisible by 19.]

$6232 = 2^3 \cdot 19 \cdot 41$

$6368 = 2^5 \cdot 199$

$\sigma(6232) - 6232 = 15 \cdot 20 \cdot 42 - 6232$

$= 12600 - 6232 = 6368$

$\sigma(6368) - 6368 = 63 \cdot 200 - 6368$

$= 12600 - 6368 = 6232$

(c) Use 168 and 297 to show that is possible to have $\sigma(m) = \sigma(n)$ without m and n being amicable.

$168 = 2^3 \cdot 3 \cdot 7$ $\qquad$ $297 = 3^3 \cdot 11$

$\sigma(168) = 15 \cdot 4 \cdot 8$ $\qquad$ $\sigma(297) = 40 \cdot 12$

$= 480$ $\qquad$ $= 486$

But $\sigma(168) - 168 = 480 - 168 = 312 \neq 297$

UNIVERSITY OF MANITOBA

DATE: March 10, 2010

MIDTERM II
PAGE: 5 of 5
TIME: 50 minutes
EXAMINER: M. Davidson

COURSE NO: MATH 2500
EXAMINATION:
Introduction to Number Theory

---

[7] 5. Given the public information of an RSA encryption key of $(n, e) = (2599, 73)$, find the decrypt key d. [Hint: One of the two prime factors of n is less than 30.]

$2599 = 23 \cdot 113$

$\phi 2599 = 22 \cdot 112 = 2464$

(want to solve $73x \equiv 1 \mod 2464$)

$2464 = 73(33) + 55$

$73 = 55(1) + 18$

$55 = 18(3) + 1$

So $1 = 55 + 18(-3)$

$= 55 + [73 + 55(-1)](-3)$

$= 73(-3) + 55(4)$

$= 73(-3) + [2464 + 73(-33)](4)$

$= 2464(4) + 73(-135)$

The decrypt key is 2329.