The University of Sydney

FACULTY OF SCIENCE

MATH2068 and MATH2988

Number Theory and Cryptography

November, 2011 Lecturer: R. B. Howlett

Time allowed: two hours

The question paper must not be removed from the examination room

No notes or books are to be taken into the examination room.
Only approved non-programmable calculators are allowed.

The MATH2068 paper has five questions.
The MATH2988 paper has one extra question (on the back page).
The questions are of equal value.

Question 6 is for MATH2988 only.

1. (*i*) Use a Vigenère cipher with keyword CAT to encrypt the plaintext message OCELOT.

(*ii*) Let $M = c_1c_2c_3 \ldots c_\ell$ be a message which is a sequence of letters from the alphabet $\{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Z}\}$.

(a) What is a *digraph*, and what is the definition of the *digraph coincidence index of M*?

(b) If the sequence M were generated by choosing successive letters independently with all letters having equal probability of being chosen each time, what would be the expected value of the digraph coincidence index?

(c) If M is ordinary English text, written in upper case letters and stripped of spacing and punctuation, would you expect the digraph coincidence index to be greater than, less than, or the same as the answer to Part (*ii*) (b)? (Give a brief reason.)

(*iii*) A long intercepted message M is reliably known to have been encrypted with a block transposition cipher. If the $(2,7)$-decimation of M with period 9 has coincidence index 0.0047 and the $(3,5)$-decimation of M of period 8 has coincidence index 0.0072, what conclusions should you draw?

2. (*i*) An *affine cipher* is a substitution cipher defined by a rule of the form

$$i \mapsto mi + n \pmod{26},$$

for some fixed integers m, n, where the letters A to Z are identified with residues modulo 26 in the usual way (A ↔ 0, B ↔ 1, etc.). The pair (m, n) is called the *key*.

(a) If the key is $(8, 16)$, encipher the message BEN.

(b) A sample of ciphertext known to have been produced by an affine cipher is found to consist of 2000 letters altogether, of which the two most common are J (271 occurrences) and N (199 occurrences). Assuming that these represent the most common letters in English, determine the key.

(*ii*) Let $n = (d_\ell d_{\ell-1} \ldots d_0)_8$; that is, when the integer n is expressed in base 8 notation its digits are d_ℓ, $d_{\ell-1}$, …, d_0.

(a) Explain what this means, and illustrate your answer by finding the base 10 representation of $n = (2145)_8$.

(b) Prove that $n \equiv d_0 + d_1 + \cdots + d_\ell \pmod{7}$.

3. (*i*) Find the order of 4 modulo each of the primes 11 and 23, and then find the residue of 4^{1112} modulo 253. (You are given that $253 = 11 \times 23$.)

(*ii*) Prove that if n, a and b are integers such that $n|ab$ and $\gcd(n, a) = 1$ then $n|b$. You may use the fact that integers r and s exist satisfying $rn + sa = \gcd(n, a)$.

(*iii*) Show that if p is a prime number and t an integer such that $t^2 \equiv 1 \pmod{p}$, then either $t \equiv 1 \pmod{p}$ or $t \equiv -1 \pmod{p}$.

4. (*i*) A user of the RSA cryptosystem has chosen $(2329127, 331)$ as the public key. Given that 2063 is a factor of 2329127, determine the private key.

(*ii*) Suppose that you are user of the Elgamal cryptosystem and that your public key is $(p, b, k) = (43, 3, 41)$ and your private key is $m = 6$.

(a) Check that the necessary relationship between the private key and the public key is satisfied.

(b) You receive the message $\langle 2, [1, 20, 21] \rangle$. Decrypt it.

(*iii*) Let $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and let a_1, a_2, a_3, ... be an infinite sequence of elements of S such that a_{i+1} is determined by a_i for every i. (That is, $a_{i+1} = f(a_i)$ for some function f from S to S.) Show that there exists a positive integer k such that $a_{2k} = a_k$.

5. (*i*) Let p be an odd prime and $n \equiv -1 \pmod{p}$. Let q be prime divisor of $N = \sum_{i=0}^{p-1} n^{ip} = 1 + n^p + n^{2p} + \cdots + n^{(p-1)p}$. Find $\operatorname{ord}_q(n)$, and then show that $q \equiv 1 \pmod{p^2}$.

(*ii*) Let p be an odd prime.

(a) Show that if k is a positive integer then $p^k \equiv 3 \pmod{4}$ if and only if $p \equiv 3 \pmod{4}$ and k is odd.

(b) Let ℓ be a positive integer and let s be the sum of the positive divisors of p^ℓ. Show that s is odd if and only if ℓ is even.

(c) Again let ℓ be a positive integer and s be the sum of the positive divisors of p^ℓ. Show that $s \equiv 2 \pmod{4}$ if and only if and $p \equiv 1 \pmod{4}$ and $\ell \equiv 1 \pmod{4}$.

(*iii*) Using Part (*ii*), show that if n is an odd perfect number then $n = p^\ell m^2$ for some integers p, ℓ and m such that p is prime and $p \equiv \ell \equiv 1 \pmod{4}$.

6. (MATH2988 students only)

(*i*) Let n be a positive integer. Prove that $\sum_{d|n} \phi(d) = n$.

(*ii*) Let $a_0 > a_1 > a_2 > \cdots > a_k$ be the successive remainders generated when the Euclidean Algorithm is used to determine $d = \gcd(a, b)$, where $(a_0, a_1) = (a, b)$ and $a_k = d$. Show that $k < 2\log_2(a) + 1$.

(*iii*) Let n be an integer greater than 1. Show that n is not a divisor of $2^n - 1$. (Consider $\mathrm{ord}_p(2)$ for prime divisors of n.)