The University of Sydney

FACULTY OF SCIENCE

MATH2068 and MATH2988

Number Theory and Cryptography

and

Number Theory and Cryptography (advanced)

November, 2010 Lecturer: A. Fish

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 (question 6).
The questions are of equal value.

Question 6 is for MATH2988 only.

1. (*i*) A Vigenère cipher with encryption key DOG is being used. If the ciphertext is VQUWHOH, find the plaintext.

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

(a) What is the definition of the *coincidence index* of M?

(b) If M is generated by independently choosing successive letters, with all 26 letters having the same probability of being chosen, what is the expected value of the coincidence index?

(c) If M is a long piece of typical English text (stripped of spacing and punctuation) approximately what value would you expect for the coincidence index?

(*iii*) Assume that text messages are encoded numerically by associating the letters A to Z (taken in alphabetical order) with the numbers 1 to 26, and using 0 to represent a blank space. Thus an encoded message is a sequence of residues modulo 27. Enciphering is performed by splitting the encoded message into blocks of length 2, and applying the formula

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 10 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 2 \\ 25 \end{pmatrix},$$

where (c,d) is the ciphertext block corresponding to the plaintext block (a,b), and all calculations are done using residue arithmetic modulo 27. Enciphered messages are converted to text by reversing the encoding process.

The enciphered message YKRP is received. Decipher it.

2. (*i*) Use the Extended Euclidean Algorithm to find integers r and s such that $752r + 103s = \gcd(752, 103)$, and hence find the inverse of 103 modulo 752.

(*ii*) Find a polynomial $f(X) = a_0 + a_1X + a_2X^2$, with coefficients a_0, a_1 and a_2 in the set $\{0,1,2,3,4\}$, satisfying $f(1) = 3$, $f(2) = 2$ and $f(4) = 2$, where all calculations are done in residue arithmetic modulo 5.

(*iii*) State the Chinese Remainder Theorem.

3. (*i*) Suppose that an RSA user's public key is $(91, 5)$.

(a) Determine the private key.

(b) Encipher the message $[5, 20]$ using the public key.

(*ii*) Let m and a be positive integers such that $\gcd(a, m) = 1$ and $1 \leq a \leq m - 1$.

(a) Use the Euler-Fermat Theorem to show that $a^{k\phi(m)+1} \equiv a \pmod{m}$ for all positive integers k.

(b) Let e, d be positive integers coprime to $\phi(m)$ and suppose that they are inverses of each other modulo $\phi(m)$. Show that if b is the residue of a^e modulo m then a is the residue of b^d modulo m.

4. (*i*) Let a, b, c, d and n be integers. Working directly from the definition of congruence modulo n, show that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.

(*ii*) Elgamal user Bill has as his public key the triple (p, b, k) where $p = 59$ and $b = 2$. His private key is $m = 6$.

(a) Find the value of k.

(b) Bill receives the message $\langle 3, [42, 7] \rangle$. Decipher it.

(*iii*) Let n be a positive integer and let p be a prime divisor of $n^{54} + n^{27} + 1$. Prove that if $p \neq 3$ then $\mathrm{ord}_p(n) = 81$, and deduce that $p \equiv 1 \pmod{81}$.

5. (*i*) For each positive integer n define $R_n = \frac{1}{9}(10^n - 1)$ (so that, in the usual base 10 notation, $R_n = 111\ldots1$, where there are n digits).

(a) Show that if R_n is prime then n must be prime.

(b) Show that if n is a prime greater than 3 and p is a prime divisor of R_n then $p \equiv 1 \pmod{n}$.

(c) Let $p = 719$ and $q = 359 = \frac{1}{2}(p - 1)$. You are given that both p and q are prime. Compute the residue of $27^2 \pmod{p}$, and use the result of this calculation to prove that R_q cannot possibly be prime.

(*ii*) Let n be a positive integer and let $N = 2^n - 1$. Show that if $2^n \equiv 2 \pmod{n}$ then $2^N \equiv 2 \pmod{N}$.

6. (MATH2988 students only)

(*i*) For each positive integer n define $F(n) = \phi(n)/\sqrt{n}$, where ϕ denotes Euler's phi function.

(a) Find all pairs of nonnegative integers a and b such that $F(2^a 3^b) < 1$.

(b) Find all positive integers n such that $F(n) < 1$.

(*ii*) Suppose that n is composite and has the property that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$.

(a) Prove that n is odd. (Consider $a = n - 1$.)

(b) Prove that n cannot be divisible by the square of a prime. (Suppose that $n = p^k m$ where p is prime, $k > 1$ and $p \nmid m$, and consider $a = (n/p) + 1$.)