The University of Sydney
FACULTY OF SCIENCE

MATH2068

Number Theory and Cryptography

November, 2008 Lecturer: R. B. Howlett

Time allowed: two hours

No notes or books are to be taken into the examination room.

Calculators will be provided; no other calculators are allowed.

The paper has five questions. The questions are of equal value.

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

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

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

(b) If M is typical English text, stripped of spacing and punctuation and written in capital letters, approximately what value would one expect for the coincidence index?

(c) 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 coincidence index?

(d) What is meant by the *decimation of M with period m and index r*?

(*iii*) An intercepted message M is reliably known to have been encrypted with a Vigenère cipher. Describe (in a few sentences) a strategy for decrypting M using decimations and coincidence indexes.

2. (*i*) Find the order of 3 modulo each of the primes 11, 13 and 19, and use the information to find the residue of 3^{2008} modulo 2717. You are given that $2717 = 11 \times 13 \times 19$.

(*ii*) Recall that the *Fibonacci numbers* F_n are defined by the rules that $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for all $n \geq 1$. Use induction to prove that for all positive integers n,

$$\begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n .$$

(*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 $t \equiv -1 \pmod{p}$.

(*iv*) Let $p = 2k + 1$ be an odd prime number and b a primitive root modulo p.

(a) Show that $b^k \equiv -1 \pmod{p}$.

(b) Recall that if n is a nonzero residue modulo p then $\log_{b,p}(n)$ is a number i such that $n \equiv b^i \pmod{p}$. Show that $n^k \equiv 1 \pmod{p}$ if $\log_{b,p}(n)$ is even, and $n^k \equiv -1 \pmod{p}$ if $\log_{b,p}(n)$ is odd.

3. (*i*) Use the extended Euclidean algorithm to find the inverse of 1541 modulo 5003. (Working must be shown.)

(*ii*) Suppose that n is a positive integer. Prove that for all integers a, b, c, d, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $ab \equiv cd \pmod{n}$.

(*iii*) Given that 658627 is the product of two distinct prime numbers and that $\phi(658627) = 657000$, find the prime factors of 658627. (Here and below ϕ denotes the Euler phi function.)

(*iv*) Suppose that an RSA user's public key is $(65, 5)$.

(a) Determine the private key.

(b) Encrypt the message $[3, 20, 4]$ using the public key.

4. (*i*) Compute the residue of 5^{11} modulo 23, and determine $\mathrm{ord}_{23}(5)$.

(*ii*) Suppose that you are a user of the Elgamal cryptosystem and that your public key is $(p, b, k) = (23, 5, 10)$ and your private key is $m = 3$.

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

(b) You receive the message $\langle 2, [7, 16, 9, 11] \rangle$. Decrypt it.

(*iii*) (a) There is a theorem that says that if a and b are positive integers then there exist integers r and s such that $ra + sb = \gcd(a, b)$. Use this to prove that if $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.

(b) Show that if $a|m$ and $b|m$ and $\gcd(a, b) = 1$ then $ab|m$.

5. (*i*) Let a and b be positive integers with $b < a$, and let c be the residue of a modulo b. Assume that $c \neq 0$, and let d the residue of b modulo c. Show that $d < \frac{1}{2}b$.

(*ii*) Suppose that n is a positive integer with $\phi(n) = 8$.

(a) Show that if p is an odd prime divisor of n then $p = 3$ or $p = 5$.

(b) Find all the possible values for n.

(*iii*) Let $p = 601$, a prime number, and let $S = \{1, 2, \ldots, 300\}$.

(a) Show that if $i \in S$ then there exist $\varepsilon \in \{1, -1\}$ and $j \in S$ such that $3i \equiv \varepsilon j \pmod{p}$.

(b) Show that if $j \in S$ then there exist $\varepsilon \in \{1, -1\}$ and $i \in S$ such that $\varepsilon j \equiv 3i \pmod{p}$.

(c) Show that if i, j and ε satisfy the conditions in Part (a) then $\varepsilon = -1$ if $101 \leq i \leq 200$, and $\varepsilon = 1$ otherwise.

(d) Show that $\prod_{i \in S} (3i) \equiv (-1)^{100} \prod_{j \in S} j$, and hence that $3^{300} \equiv 1 \pmod{p}$.

End of Examination Paper