8038 Semester 2 2007

The University of Sydney

FACULTY OF SCIENCE

MATH2068

Number Theory and Cryptography

November, 2007

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.

. . . /2

1. (*i*) Given that $455 = 5 \times 7 \times 13$, find the residue of 3^{2007} modulo 455. (Start by finding the order of 3 modulo each of the primes 5, 7 and 13.)

(*ii*) Use the extended Euclidean algorithm to find the inverse of 1237 modulo 3767. (Working must be shown.)

(*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

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 20 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 19 \\ 3 \end{pmatrix},$$

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 transmitted as text by reversing the encoding process.

The enciphered message AWDL is received. Decipher it.

2. (*i*) Find four positive integers x less than 1829 such that $x^2 \equiv 5 \pmod{1829}$. You are given that 1829 is the product of 31 and 59.

(*ii*) A user of the RSA cryptosystem has $(1216573, 257)$ as his public key. Given that 1109 is a factor of 1216573, use your calculator to verify that his private key is $(1216573, 1186017)$. (You must write down the steps you use and the results of any intermediate calculations.)

(*iii*) Use the Lagrange interpolation formula to find a quadratic polynomial $f(x)$ with integer coefficients such that the following congruences all hold:

$$\begin{aligned} f(0) &\equiv 2 \pmod{11}, \\ f(2) &\equiv 6 \pmod{11}, \\ f(7) &\equiv 3 \pmod{11}. \end{aligned}$$

3. (*i*) 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 $ab \equiv cd \pmod{n}$.

(*ii*) Let p be a prime divisor of $10^{256}+1$. By considering $\mathrm{ord}_p(10)$, prove that $p-1$ is divisible by 512.

(*iii*) (a) The number 641 is prime. What does Fermat's Little Theorem tell us about $\mathrm{ord}_{641}(2)$?

(b) Check that $5 \times 2^7 \equiv -1 \pmod{641}$ and $5^4 \equiv -2^4 \pmod{641}$, and then use these congruences to prove that $\mathrm{ord}_{641}(2) = 64$.

(*iv*) Given that $11^3 = 1331$, find all prime numbers p such that $\mathrm{ord}_p(11) = 3$.

4. (*i*) It follows from the extended Euclidean Algorithm that if a and b are any two integers then there exist integers s and t such that $sa+tb = \gcd(a,b)$. Use this to prove that if a, b and c are integers such that a and b are coprime and $a|bc$ then $a|c$.

(*ii*) Suppose that a and b are coprime integers and n is an integer such that $a|n$ and $b|n$. Prove that $ab|n$.

(*iii*) Suppose that you are user of the Elgamal cryptosystem and that your public key is $(p,b,k) = (59,10,54)$ and your private key is $m = 5$.

(a) Check that the necessary relationship between the private key and the public key is indeed satisfied. (It is given that 10 is a primitive root modulo 59; you need not check this.)

(b) You receive the message $\langle 2, [3,2,32] \rangle$. Decipher it.

5. (*i*) Let p be an odd prime. Show that the $p-3$ numbers from 2 to $p-2$ can be paired up in such a way that the product of each pair is congruent to 1 modulo p, and use this to deduce that $(p-2)! \equiv 1 \pmod{p}$.

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

(a) Show that if k 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 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, and $s \equiv 2 \pmod{4}$ if and only if and $p \equiv 1 \pmod{4}$ and $\ell \equiv 1 \pmod{4}$.

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