The University of Sydney
FACULTY OF SCIENCE

MATH2068 and MATH2988

Number Theory and Cryptography

November, 2012 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.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

1. (*i*) Find $i \in \{0, 1, \ldots, 384\}$ which satisfies that $i \equiv 3 \pmod 5$, $i \equiv 6 \pmod 7$, and $i \equiv 2 \pmod{11}$ (Use the fact that $385 = 5 * 7 * 11$).

(*ii*) By use of Euclidean algorithm find $\gcd(234, 569)$.

(*iii*) (a) Give the definition of a square modulo a prime p.

(b) Find all non-zero squares modulo 17.

2. (*i*) A Vigenère cipher with encryption key KEY is being used. If the ciphertext is QSMNPSMO, find the plaintext.

(*ii*) 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

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} 2 \\ 11 \end{pmatrix},$$

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 OXPD is received. Decipher it.

(*iii*) Let $n = (d_\ell d_{\ell-1} \ldots d_0)_9$; that is, when the integer n is expressed in base 9 notation its digits are d_ℓ, $d_{\ell-1}$, $\ldots$, d_0.

(a) Explain what this means, and illustrate your answer by finding the base 10 representation of $n = (2135)_9$.

(b) Prove that $n \equiv d_0 + d_1 + \cdots + d_\ell \pmod 4$.

3. (*i*) (a) Define the notion of order of a number b modulo n ($\text{ord}_n(b)$), given that $\gcd(b, n) = 1$.

(b) Prove that $\text{ord}_n(b)|\phi(n)$.

(*ii*) Prove that if a and b are relatively prime integers, i.e. $\gcd(a, b) = 1$, then a^2 and b^2 are also relatively prime.

(*iii*) Show that if p is a prime number and t an integer such that $t^2 \equiv 4 \pmod{p}$, then either $t \equiv 2 \pmod{p}$ or $t \equiv -2 \pmod{p}$.

4. (*i*) Suppose that an RSA user's public key is $(77, 43)$.

(a) Determine the private key.

(b) Decipher the message $[8, 12]$.

(*ii*) Suppose that you are user of the Elgamal cryptosystem and that your public key is $(p, b, k) = (37, 3, 21)$ and your private key is $m = 5$.

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

(b) You receive the message $\langle 5, [1, 20, 21] \rangle$. Decrypt it.

(*iii*) (a) Give the definition of Möbius function $\mu(n)$.

(b) Check that

$$\sum_{n|900} \frac{\mu(n)}{n} = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right).$$

(c) Prove that if N is any positive integer then

$$\sum_{n|N} \frac{\mu(n)}{n} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right),$$

where $p_1, p_2, \ldots, p_k$ are all the prime factors of N.

5. (*i*) Let p be an odd prime. Prove that if $2^p \equiv 1 \pmod{(2p+1)}$ then $2p + 1$ is a prime.

(*ii*) Let p be an odd prime. Prove that $(p - 3)! \equiv \frac{p-1}{2} \pmod{p}$.

6. (MATH2988 students only)

(i) Let p be an odd prime, and k a positive integer not divisible by $p-1$. Show that

$$1^k + 2^k + \ldots + (p-1)^k \equiv 0 \pmod{p}.$$

(ii) Prove that the number of primitive roots modulo p (p is a prime) is equal to $\phi(p-1)$.

(iii) Prove that there are no rational solutions for the equation $x^2 + y^2 = 3$.