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.

Solution: (i) $i \equiv 3 \pmod 5$ implies $i = 3 + 5k$, then plugging that into $i \equiv 6 \pmod 7$ implies $3 + 5k \equiv 6 \pmod 7$, which implies that $5k \equiv 3 \pmod 7$. This implies that $k \equiv 2 \pmod 7$. Thus we have $i = 3+5(7\ell+2) = 13+35\ell$. Plugging that into the last identity we get $13 + 35\ell \equiv 2 \pmod{11}$. This is the same as $35\ell \equiv 0 \pmod{11}$. The latter implies that $\ell = 11m$. Eventually we get $i = 13 + 35 \times 11m$. Thus $i = 13$ is the solution.

(ii) $\gcd(234, 569) = \gcd(234, 569 - 2 \cdot 234) = \gcd(234, 101)$

$$= \gcd(234 - 2 \cdot 101, 101) = \gcd(32, 101) = \gcd(32, 101 - 3 \cdot 32)$$

$$= \gcd(32, 5) = \gcd(32 - 6 \cdot 5, 5) = \gcd(2, 5)$$

$$= \gcd(2, 1) = \gcd(1, 1) = 1$$

(iii) (a) A number $n \in \mathbb{Z}_p$ is a square modulo p, if there exists $k \in \mathbb{Z}$ such that $k^2 \equiv n$ (mod p).

(b) To find all non-zero squares modulo 17 it is enough to find the residues modulo 17 of $1^2, \ldots, 8^2$, namely $1, 4, 9, 16, 8, 2, 15, 13$.

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 $n = (d_\ell d_{\ell-1} \dots d_0)_9$; that is, when the integer n is expressed in base 9 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 $n = (2135)_9$.

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

Solution: (*i*) The plaintext is GOODLUCK.

(*ii*) The plaintext is MATH.

(*iii*) (a) $n = (d_\ell d_{\ell-1} \dots d_0)_9$ means $n = \sum_{k=0}^{\ell} d_k 9^k$. In the case $n = (2135)_9$ it means $n = 5 + 3 \cdot 9 + 1 \cdot 9^2 + 2 \cdot 9^3 = 1571$

(b) It is enough to prove that $4 | n - (d_0 + \ldots + d_\ell)$. But

$$n - (d_0 + \ldots + d_\ell) = \sum_{k=0}^{\ell} (9^k - 1) \cdot d_k.$$

Here every term is divisible by 4, since $9^k \equiv 1 \pmod 4$, so we obtain the claim.

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

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

(*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 $t \equiv -2 \pmod{p}$.

Solution: (*i*) (a) $\mathrm{ord}_n(b) = \min\{k \geq 1 | b^k \equiv 1 \pmod{n}\}$. By the Euler–Fermat theorem this is well defined in the case $\gcd(b,n)=1$.

(b) We know by Euler-Fermat theorem that $b^{\phi(n)} \equiv 1 \pmod{n}$. By the definition of the order it follows that $\mathrm{ord}_n(b) \leq \phi(n)$. Let $\phi(n) = q\,\mathrm{ord}_n(b) + r$, where $0 \leq r < \mathrm{ord}_n(b)$. Then by plugging $\phi(n)$ into the identity $b^{\phi(n)} \equiv 1 \pmod{n}$ we get $b^r \equiv 1 \pmod{n}$. This would contradict the definition of the order, if $r \geq 1$. Thus $r=0$, which implies $\mathrm{ord}_n(b)|\phi(n)$.

(*ii*) If $\gcd(a^2,b^2) > 1$ then there exists a prime p such that $p|a^2$ and $p|b^2$. Since the latter implies that $p|a$ and $p|b$ we get that $p|\gcd(a,b)$. In particular, $\gcd(a,b) \geq p > 1$, contrary to assumption.

(*iii*) If $t \in \mathbb{Z}$ satisfies the identity $t^2 \equiv 4 \pmod{p}$ this implies that t is a zero of the polynomial x^2-4 over $\mathbb{Z}_p$. But $x^2-4=(x-2)(x+2)$. Therefore any root t of this polynomial is 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.

Solution: (*i*) (a) $m = 77 = 7 \cdot 11$. Therefore $\phi(m) = 6 \cdot 10 = 60$. If a number $e = 43$ is a public key of the RSA system, then the private key d is the inverse of e modulo $\phi(m)$. I.e. $e \cdot d \equiv 1 \pmod{60}$. But $43 \cdot 7 \equiv 1 \pmod{60}$. Thus $d = 7$.

(b) The sent message is $[8^d \pmod{77}, 12^d \pmod{77}] = [57, 12]$.

(*ii*) (a) The condition is that $k \equiv b^m \pmod{p}$, so we check that, modulo 37,

$$3^5 \equiv 81 \times 3 \equiv 7 \times 3 \equiv 21.$$

(b) To decrypt a message in Elgamal, recall that $c \equiv b^i$ (mod p), and $N_j \equiv k^i M_j$ (mod p), where i is a randomly chosen number by a sender of a message and M_j is the jth residue of the plaintext of the message. We have $c = 5$, $N_1 = 1, N_2 = 20, N_3 = 21$. To decrypt the message we just have to find $c^m \equiv k^i$(mod p) first. In our case $c^m \equiv 17 \pmod{37}$. Next we have to invert 17 modulo 37. This is easy and the result is 24. Then $M_j \equiv 24 \times N_j$ (mod p). In our case we have $M_1 \equiv 1 \times 24 \equiv 24$, $M_2 \equiv 20 \times 24 \equiv 36$, $M_3 \equiv 21 \times 24 \equiv 23 \pmod{37}$. So the plaintext is $[24, 36, 23]$.

(*iii*) (a) $\mu(n)$ is equal to 1 if n is square free and the number of prime divisors of n is even, it is equal to -1 if n is square free and the number of prime divisors of n is odd, and it is equal to zero if n is non square free. Also $\mu(1) = 1$.

(b) Since $900 = 3^2 \times 2^2 \times 5^2$, the divisors of 900 are either non-square free, or they are $1, 2, 3, 5, 2 \times 3, 2 \times 5, 3 \times 5, 2 \times 3 \times 5$. Thus

$$\sum_{n|900} \frac{\mu(n)}{n} = 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2 \times 3} + \frac{1}{2 \times 5} + \frac{1}{3 \times 5} - \frac{1}{2 \times 3 \times 5}$$

$$= \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

(c) Define

$$F(N) = \sum_{n|N} \frac{\mu(n)}{n}.$$

Since $\mu(n)$ is a multiplicative function, so is $\frac{\mu(n)}{n}$. By a result in lectures, we can conclude that F is a multiplicative function. Now if $N = p^a$ where p is prime and a is a positive integer, we have

$$F(p^a) = \frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^a)}{p^a} = 1 - \frac{1}{p},$$

since p^i is not square free when $i \geq 2$. So for a general positive integer N with prime factorization $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, we have

$$F(N) = F(p_1^{a_1}) \cdots F(p_k^{a_k}) = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

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

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

Solution: (*i*) If $2p+1$ is non-prime, then there is $q < p$ a prime which divides $2p+1$. Then $2^p \equiv 1 \pmod{q}$. This implies that $\mathrm{ord}_q(2)|p$. Since p is a prime it implies that $\mathrm{ord}_q(2) = p$. But by Fermat's little theorem we have that $\mathrm{ord}_q(2) \leq q-1$. We get a contradiction.

(*ii*) Let b be a primitive root modulo p. Then

$$(p-3)!(p-2)(p-1) \equiv \prod_{k=1}^{p-1} b^k \equiv b^{\frac{p(p-1)}{2}} = (b^p)^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1$$

(mod p). The last identity is because b is a primitive root. Thus $(p-3)!$ is an inverse to $p-2$ modulo p. But $\frac{p-1}{2} \times (p-2) \equiv p\frac{p-3}{2} + 1 \equiv 1 \pmod{p}$, so $\frac{p-1}{2}$ is also an inverse to $p-2$ modulo p. Since inverses are unique up to congruence, the claim follows.

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 $x^2 + y^2 = 3$.

Solution: (i) Let b a primitive root modulo p. Then the LHS is congruent mod p to $1+b^k+b^{2k}+\ldots+b^{(p-2)k} = B$, say. We have $B(1-b^k) = 1-(b^k)^{p-1} \equiv 0 \pmod{p}$ by Fermat's little theorem. Since k is not divisible by $p-1$, $1-b^k \not\equiv 0 \pmod{p}$, so we can conclude that $B \equiv 0 \pmod{p}$ as desired.

(ii) Denote by $F(d)$ the number of residues modulo p which have order d. We know that $F(d)$ can be non-zero only for $d \,|\, p-1$. For every $e \,|\, p-1$, the total number of residues x modulo p such that $x^e \equiv 1 \pmod{p}$ is e, so $\sum_{d|e} F(d) = e$ for every $e \,|\, p-1$. By the Möbius inversion formula there is a unique function F on divisors of $p-1$ which satisfies $\sum_{d|e} F(d) = e$ for every $e \,|\, p-1$. But we also know that ϕ satisfies $\sum_{d|e} \phi(d) = e$ for all e. Therefore $F(d) = \phi(d)$ for all $d \,|\, p-1$. The number of primitive roots modulo $p-1$ is exactly equal to $F(p-1)$. Therefore it is equal to $\phi(p-1)$.

(iii) Assume for a contradiction that $\frac{m}{n}, \frac{p}{n}$ are two rational numbers which are a solution of the equation, i.e. $m^2+p^2 = 3n^2$. We can assume that there is no common divisor of m, p, n greater than 1, because if $d > 1$ divided all of m, p, n then we could replace m, p, n by $m/d, p/d, n/d$ to get another such triple. Since the squares modulo 3 are 0 and 1, and $3n^2 \equiv 0 \pmod{3}$, it must be that both m and p are divisible by 3. Therefore $m = 3m'$, $p = 3p'$ for some integers m', p'. Then we have $3(m'^2 + p'^2) = n^2$. Therefore n also is divisible by 3. We have obtained our desired contradiction.