INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Stamp / Signature of the Invigilator

EXAMINATION (End Semester)										**SEMESTER (Spring)**			
Roll Number										**Section**		**Name**	
Subject Number	C	S	6	0	0	9	4	**Subject Name**		*Computational Number Theory*			
Department / Center of the Student											**Additional sheets**		

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as **'unfair means'**. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Marks Obtained											

Marks obtained (in words)	**Signature of the Examiner**	**Signature of the Scrutineer**

CS60094 Computational Number Theory, Spring 2016–2017

End-Semester Test

26–April–2017 CSE-107/119/120, 02:00–05:00pm Maximum marks: 75

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. Represent the finite field $\mathbb{F}_{16} = \mathbb{F}_{2^4} = \mathbb{F}_2(\theta)$ with $\theta^4 + \theta + 1 = 0$. Let $\alpha = \theta + 1$.

(a) Check whether α is a primitive element (a generator of $\mathbb{F}_{16}^*$). **(5)**

Solution We have $|\mathbb{F}_{16}^*| = 15 = 3 \times 5$. It suffices to check that $\alpha \neq 1$, $\alpha^3 = \theta^3 + \theta^2 + \theta + 1 \neq 1$, and $\alpha^5 = (\theta^4 + 1)(\theta + 1) = \theta(\theta + 1) = \theta^2 + \theta \neq 1$ to conclude that α is a primitive element of $\mathbb{F}_{16}^*$.

(b) Check whether α is a normal element of $\mathbb{F}_{16}$ (over $\mathbb{F}_2$). **(5)**

Solution We have $\alpha = 1 + \theta$, $\alpha^2 = 1 + \theta^2$, $\alpha^4 = 1 + \theta^4 = \theta$, and $\alpha^8 = \theta^2$, that is,

$$\begin{pmatrix} \alpha \\ \alpha^2 \\ \alpha^4 \\ \alpha^8 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \theta^2 \\ \theta^3 \end{pmatrix}.$$

Since the last column of the transformation matrix contains only zeros, the matrix is singular, and so α is not a normal element.

(c) Compute the minimal polynomial of α over $\mathbb{F}_2$. **(5)**

Solution Since $\theta = \alpha^4$, α is a conjugate of θ, so the minimal polynomial of α is the same as the minimal polynomial of θ, that is, x^4+x+1. This can also be verified by direct calculations:

$$\begin{aligned}
& (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8) \\
= \; & (x+1+\theta)(x+1+\theta^2)(x+\theta)(x+\theta^2) \\
= \; & \left(x^2+(\theta+\theta^2)x+(1+\theta+\theta^2+\theta^3)\right)\left(x^2+(\theta+\theta^2)x+\theta^3\right) \\
= \; & x^4+(\theta^2+\theta^4)x^2+(x^2+(\theta+\theta^2)x)(1+\theta+\theta^2)+(\theta^3+\theta^4+\theta^5+\theta^6) \\
= \; & x^4+(\theta^4+\theta+1)x+(\theta+\theta^2)(1+\theta+\theta^2)x+(\theta^2+\theta^4+\theta^5) \\
= \; & x^4+(\theta+\theta^2+\theta^2+\theta^4)x+(\theta+\theta^4) \\
= \; & x^4+x+1.
\end{aligned}$$

2. Charlier polynomials $C_i(x)$ modulo 2 are defined recursively as follows.

$$\begin{aligned} C_0(x) &= 1, \\ C_i(x) &= \begin{cases} xC_{i-1}(x) & \text{if } i \text{ is odd,} \\ (x+1)C_{i-1}(x) & \text{if } i \text{ is even,} \end{cases} \qquad \text{for } i \geqslant 1. \end{aligned}$$

(a) For $i, j \geqslant 0$, prove that

$$C_i(x)C_j(x) = \begin{cases} C_{i+j}(x) & \text{if at least one of } i \text{ and } j \text{ is even,} \\ C_{i+j}(x) + C_{i+j-1}(x) & \text{if both } i \text{ and } j \text{ are odd.} \end{cases} \qquad \textbf{(10)}$$

Solution For every $r \geqslant 0$, we have $C_{2r}(x) = x^r(1+x)^r$ and $C_{2r+1}(x) = x^{r+1}(x+1)^r$. We now consider several cases.

Case 1: $i = 2r$ and $j = 2s$.

$C_i(x)C_j(x) = x^r(1+x)^r x^s(1+x)^s = x^{r+s}(1+x)^{r+s} = C_{2(r+s)}(x) = C_{i+j}(x)$.

Case 2: $i = 2r$ and $j = 2s+1$.

$C_i(x)C_j(x) = x^r(1+x)^r x^{s+1}(1+x)^s = x^{r+s+1}(1+x)^{r+s} = C_{2(r+s)+1}(x) = C_{i+j}(x)$.

Case 3: $i = 2r+1$ and $j = 2s$.

$C_i(x)C_j(x) = x^{r+1}(1+x)^r x^s(1+x)^s = x^{r+s+1}(1+x)^{r+s} = C_{2(r+s)+1}(x) = C_{i+j}(x)$.

Case 4: $i = 2r+1$ and $j = 2s+1$.

$C_i(x)C_j(x) = x^{r+1}(1+x)^r x^{s+1}(1+x)^s = x^{r+s+2}(1+x)^{r+s} = (1+x)x^{r+s+1}(1+x)^{r+s} + x^{r+s+1}(1+x)^{r+s} = C_{2(r+s+1)}(x) + C_{2(r+s)+1}(x) = C_{i+j}(x) + C_{i+j-1}(x)$.

(b) Represent $\mathbb{F}_{2^n} = \mathbb{F}_2(\theta)$, where $f(\theta) = 0$ for an irreducible polynomial $f(x) \in \mathbb{F}_2[x]$ of degree n. Prove that $C_0(\theta), C_1(\theta), C_2(\theta), \ldots, C_{n-1}(\theta)$ form an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^n}$. **(5)**

Solution $C_i(x)$ is a (monic) polynomial of degree equal to i. If we write

$$\begin{pmatrix} C_0(\theta) \\ C_1(\theta) \\ C_2(\theta) \\ \vdots \\ C_{n-1}(\theta) \end{pmatrix} = T \begin{pmatrix} 1 \\ \theta \\ \theta^2 \\ \vdots \\ \theta^{n-1} \end{pmatrix},$$

the transformation matrix T is lower triangular with the main diagonal consisting only of ones. Therefore $\det T = 1$, and the result follows.

(c) Propose an efficient algorithm to convert an element $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \in \mathbb{F}_{2^n}$ in the polynomial-basis representation to the Charlier-basis representation $\alpha = b_0C_0(\theta) + b_1C_1(\theta) + b_2C_2(\theta) + \cdots + b_{n-1}C_{n-1}(\theta)$. **(5)**

Solution We precompute $C_0(\theta), C_1(\theta), C_2(\theta), \ldots, C_{n-1}(\theta)$ in the polynomial basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$. The conversion algorithm proceeds as follows.

For $i = n-1, n-2, \ldots, 1, 0$ **(in that order), repeat:**
  If the coefficient of θ^i **in** α **is** 1,
    take $b_i = 1$, **and**
    update $\alpha := \alpha + C_i(\theta)$,
  else
    take $b_i = 0$.
Return $(b_0, b_1, b_2, \ldots, b_{n-1})$.

The running time of this algorithm is $O(n^2)$.

(**Remark:** Akleylek, Cenk, and Özbudak (INDOCRYPT 2010) propose an efficient implementation of $\mathbb{F}_{2^n}$ arithmetic using Charlier bases. Multiplication involves the use of the formula in Part (a). Reduction becomes efficient if irreducible Charlier binomials ($f(x) = C_n(x) + C_0(x)$) or trinomials ($f(x) = C_n(x) + C_k(x) + C_0(x)$) are available.)

3. Let p, q be odd primes, $n = pq$, $a \in \mathbb{Z}_n^*$, and $d = \gcd(p-1, q-1)$.

(a) Prove that n is a (Fermat) pseudoprime to base a if and only if $a^d \equiv 1 \pmod{n}$. **(10)**

Solution [If] This follows from the fact that $n-1 = pq-1 = pq-p+p-1 = p(q-1)+(p-1)$ is a multiple of d.

[Only if] Let $h = \mathrm{ord}_n(a)$. Since h divides $n-1$ and $\phi(n)$, h divides $n-1-\phi(n) = pq-1-(p-1)(q-1) = p+q-2 = (p-1)+(q-1)$, that is, $a^{p-1}a^{q-1} \equiv 1 \pmod{n}$. Reduction modulo q gives $a^{p-1} \equiv 1 \pmod{q}$. We also have $a^{p-1} \equiv 1 \pmod{p}$. It follows that $a^{p-1} \equiv 1 \pmod{n}$, that is, $h|(p-1)$. Likewise, $h|(q-1)$.

(b) Prove that n is a pseudoprime to exactly d^2 bases in $\mathbb{Z}_n^*$. **(5)**

Solution Since $d|(p-1)$, the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions. Likewise, the congruence $x^d \equiv 1 \pmod{q}$ has exactly d solutions. Combining using the CRT gives exactly d^2 solutions of $x^d \equiv 1 \pmod{n}$.

(c) To how many bases in $\mathbb{Z}_n^*$ is n a pseudoprime if

(i) $q = 2p-1$,
(ii) $q = 2p+1$? **(5)**

Solution (i) We have $d = \gcd(p-1, q-1) = \gcd(p-1, 2(p-1)) = p-1$, so the count of bases to which n is a pseudoprime is $d^2 = (p-1)^2 = \phi(n)/2$.

(ii) In this case, $d = \gcd(p-1, q-1) = \gcd(p-1, 2p) = 2$, so the desired count is $d^2 = 4$.

4. In the original QSM, we took $T(c) = (H+c)^2 - n = J + 2cH + c^2$ (where $H = \lceil \sqrt{n} \rceil$ and $J = H^2 - n$). Let us instead choose c_1, c_2 satisfying $-M \leqslant c_1 \leqslant c_2 \leqslant M$, and consider $T(c_1, c_2) = (H+c_1)(H+c_2) - n = J + (c_1+c_2)H + c_1c_2$.

(a) Describe how we get a relation in this variant of the QSM. **(5)**

Solution The factor base B consists of -1, the first t primes $p_1, p_2, \ldots, p_t$, and the $2M+1$ integers $H+c$. If some $T(c_1,c_2) = (-1)^\delta p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}$ is smooth over the first t primes, we get the relation

$$1^2 \equiv (-1)^\delta p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} (H+c_1)^{-1} (H+c_2)^{-1} \pmod{n}.$$

(b) Prove that if we choose $t = L[1/2]$ primes in the factor base and $M = L[1/2]$, we expect to obtain the required number of relations. **(5)**

Solution Since $|T(c_1,c_2)|$ values are roughly $O(\sqrt{n})$, each such $T(c_1,c_2)$ is smooth with respect to $L[1/2]$ primes with probability $L[-1/2]$. The factor base consists of $L[1/2]$ elements. The total number of pairs (c_1,c_2) satisfying $-M \leqslant c_1 \leqslant c_2 \leqslant M$ is $(2M+1) + 2M + (2M-1) + \cdots + 2 + 1 = M(2M+1) \approx 2M^2 = L[1]$. Therefore we expect $L[-1/2] \times L[1] = L[1/2]$ relations, as desired.

(c) Describe a sieving procedure for this variant of the QSM. **(5)**

Solution For each fixed c_1, we run a sieve indexed by c_2 in the range $c_1 \leqslant c_2 \leqslant M$. We initialize the sieve array as $A[c_2] = \log|T(c_1,c_2)|$. Let p be a small prime in B, and h a small exponent. The condition $p^h|T(c_1,c_2)$ implies $(H+c_1)c_2 \equiv -(J+c_1H) \pmod{p^h}$. For each solution χ of this linear congruence, we subtract $\log p$ from $A[c_2]$ for all $c_2 \in [c_1,M]$ satisfying $c_2 \equiv \chi \pmod{p^h}$. When all (p,h) pairs are handled, we locate those c_2 for which $A[c_2] \approx 0$. The corresponding relations are obtained by factoring $T(c_1,c_2)$ using trial division by the small primes.

(d) Argue that this variant of the QSM can be implemented to run in $L[1]$ time. **(5)**

Solution We first show that each sieve can be finished in $L[1/2]$ time. Initializing A takes $\log^2 n L[1/2]$ time, which is again of the form $L[1/2]$. Let us now look at the congruence $(H+c_1)c_2 \equiv -(J+c_1H) \pmod{p^h}$. If this congruence has no solutions, no log values are subtracted. If this congruence has a unique solution, $\log p$ is subtracted about $(2M+1)/p^h$ times. Since $p^h \leqslant n$, summing over all pairs (p,h) imply a total cost of $\leqslant (2M+1)\sum_{i=1}^{n} \frac{1}{i} \approx 2M \ln n$, which is again an expression of the form $L[1/2]$. A problematic case is when the congruence $(H+c_1)c_2 \equiv -(J+c_1H) \pmod{p^h}$ has multiple solutions. In this case, we may have to subtract $\log p$ from too many locations in A. Notice, however, that $T(c_1,c_2)$ cannot have more than $\log_2 n$ prime factors. So this bad situation arises in at most $\log_2 n$ cases. Even if we subtract log values from all locations in A in all these cases, this implies a total effort of $(2M+1)\log_2 n$, which is again $L[1/2]$.

We have to run $L[1/2]$ sieves for $2M+1$ values of c_1. Therefore the relation-collection phase takes a total of $L[1/2] \times L[1/2] = L[1]$ time. Finally, the linear-algebra phase using a sparse-system solver can be finished in $L[1/2]^2 = L[1]$ time.