INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Stamp / Signature of the Invigilator

EXAMINATION (Mid 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

Mid-Semester Test

17–February–2017 CSE-107/119/120, 02:00–04:00pm Maximum marks: 40

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

1. Let m be a large modulus, and $a, b \in \mathbb{Z}_m$. A sequence $x_0, x_1, x_2, \ldots$ is defined by first choosing some $x_0 \in \mathbb{Z}_m$, and then recursively assigning $x_n \equiv ax_{n-1} + b \pmod{m}$ for $n \geqslant 1$. Assume that $a - 1$ is invertible modulo m. Propose an algorithm to compute x_n in time polynomial in both $\log m$ and $\log n$. **(8)**

Solution Let us unwind the recurrence to get

$$\begin{aligned} x_n &\equiv ax_{n-1} + b \\ &\equiv a(ax_{n-2} + b) + b \\ &\equiv a^2 x_{n-2} + (a+1)b \\ &\equiv a^2(ax_{n-3} + b) + (a+1)b \\ &\equiv a^3 x_{n-3} + (a^2 + a + 1)b \\ &\cdots \\ &\equiv a^n x_0 + (a^{n-1} + \cdots + a^2 + a + 1)b \\ &\equiv a^n x_0 + (a-1)^{-1}(a^n - 1)b \pmod{m}. \end{aligned}$$

Using a square-and-multiply exponentiation algorithm, we can compute $a^n \pmod{m}$ in $\text{poly}(\log n, \log m)$ time. The remaining operations (inverse, multiplication, and addition modulo m) can be completed in $\text{poly}(\log m)$ time.

2. Let an irrational number ξ have the infinite simple continued fraction expansion $\langle a_0, a_1, a_2, \ldots \rangle$. Recall that the n-th convergent of ξ is the rational number $r_n = \dfrac{h_n}{k_n} = \langle a_0, a_1, a_2, \ldots, a_n \rangle$ for $n \geqslant 0$. Prove that the n-th convergent of the golden ratio $\rho = \dfrac{1+\sqrt{5}}{2}$ is $\dfrac{F_{n+2}}{F_{n+1}}$, where F_i is the i-th Fibonacci number ($F_0 = 0$, $F_1 = 1$, and $F_i = F_{i-1} + F_{i-2}$ for $i \geqslant 2$). **(8)**

Solution Let us first compute the infinite simple continued fraction expansion of ρ as follows:

$$\rho_0 = \rho = \frac{1+\sqrt{5}}{2} = 1.618\ldots, \quad a_0 = \lfloor \rho_0 \rfloor = 1,$$
$$\rho_1 = \frac{1}{\rho_0 - a_0} = \frac{2}{-1+\sqrt{5}} = \frac{2(1+\sqrt{5})}{-1+5} = \frac{1+\sqrt{5}}{2} = 1.618\ldots, \quad a_1 = \lfloor \rho_1 \rfloor = 1,$$
$$\ldots$$

It follows that $\rho = \langle 1, 1, 1, \ldots \rangle = \langle \overline{1} \rangle$. We now prove by induction on n that

$$r_n = \langle \underbrace{1, 1, \ldots, 1}_{n+1 \text{ times}} \rangle = \frac{F_{n+2}}{F_{n+1}}$$

for all $n \geqslant 0$. For $n = 0$, we have

$$r_0 = \langle 1 \rangle = 1 = \frac{1}{1} = \frac{F_2}{F_1}.$$

Suppose that the result holds for $n-1$. We then have

$$r_n = 1 + \frac{1}{r_{n-1}} = 1 + \frac{F_n}{F_{n+1}} = \frac{F_{n+1} + F_n}{F_{n+1}} = \frac{F_{n+2}}{F_{n+1}}.$$

3. (a) Prove that the polynomial $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_5[x]$. **(4)**

Solution A cubic polynomial is reducible over $\mathbb{F}_5$ if and only if it has a root in $\mathbb{F}_5$. But $f(0) \equiv 1 \pmod 5$, $f(1) \equiv 3 \pmod 5$, $f(2) \equiv 11 \equiv 1 \pmod 5$, $f(3) \equiv 31 \equiv 1 \pmod 5$, and $f(4) \equiv 69 \equiv 4 \pmod 5$.

(b) Let θ be an imaginary root of $f(x)$. Define the extension $\mathbb{F}_{5^3} = \mathbb{F}_5(\theta) = \{a\theta^2 + b\theta + c \mid a,b,c \in \mathbb{F}_5\}$. Let $\alpha = \theta^2 + 1$ and $\beta = 2\theta^2 + 3\theta + 4$ be elements of $\mathbb{F}_{5^3}$ in this representation. Compute $\alpha + \beta$, $\alpha\beta$, and α^{-1} as elements of $\mathbb{F}_{5^3}$ in the above representation. **(8)**

Solution We have

$$\alpha + \beta = 3\theta^2 + 3\theta + 5 = 3\theta^2 + 3\theta,$$

and

$$\begin{aligned}
\alpha\beta &= \theta^2(2\theta^2 + 3\theta + 4) + (2\theta^2 + 3\theta + 4) \\
&= 2\theta^4 + 3\theta^3 + 6\theta^2 + 3\theta + 4 \\
&= 2\theta^4 + 3\theta^3 + \theta^2 + 3\theta + 4 \\
&= -2\theta(\theta + 1) - 3(\theta + 1) + \theta^2 + 3\theta + 4 \\
&= -\theta^2 - 2\theta + 1 \\
&= 4\theta^2 + 3\theta + 1.
\end{aligned}$$

Solution *(continued)* We can compute α^{-1} by first noting that

$$0 = \theta^3 + \theta + 1 = \theta\alpha + 1.$$

It follows that

$$\alpha^{-1} = -\theta = 4\theta.$$

4. Counting points on curves defined over finite fields is an interesting and important computational problem. For simple curves, however, these counts can be derived mathematically. Let p be a large prime.

(a) Show that the straight line $ax + by \equiv c \pmod{p}$ (where a and b are not both zero modulo p) has exactly p solutions for (x, y). **(4)**

Solution First, assume that a is non-zero modulo p, that is, $\gcd(a, p) = 1$. But then, for each value of $y \in \mathbb{Z}_p$, there is a unique solution for x satisfying the congruence $ax \equiv c - by \pmod{p}$. If $a \equiv 0 \pmod{p}$, then b must be non-zero modulo p, that is, $by \equiv c \pmod{p}$ has a unique solution $k \equiv b^{-1}c \pmod{p}$. But then, (h, k), $h \in \mathbb{Z}_p$, are all the points on the line.

(b) Let $p \equiv 1 \pmod 4$, and $a \in \mathbb{Z}_p^*$. Show that the circle $x^2 + y^2 \equiv a \pmod p$ has exactly $p-1$ points (x,y). (**Hint:** Let $r^2 \equiv -1 \pmod p$. Rewrite the equation of the circle as $(x+ry)(x-ry) \equiv a \pmod p$.) **(4)**

Solution Since $p \equiv 1 \pmod 4$, we have $\left(\frac{-1}{p}\right) = +1$. Let r be a square root of -1 modulo p, that is, $r^2 \equiv -1 \pmod p$. So the equation of the circle can be rewritten as $x^2 - (ry)^2 \equiv a \pmod p$. Introducing two new variables u, v satisfying $u \equiv x + ry \pmod p$ and $v \equiv x - ry \pmod p$ further rewrites the equation of the circle as $uv \equiv a \pmod p$. Since $a \in \mathbb{Z}_p^*$, this congruence is not solvable if we put $u \equiv 0 \pmod p$. But for any $u \in \mathbb{Z}_p^*$, we get a unique solution for $v \equiv u^{-1}a \pmod p$. Finally, for each solution u, v, we get a unique solution $x \equiv 2^{-1}(u+v) \pmod p$ and $y \equiv (2r)^{-1}(u-v) \pmod p$.

(c) Let $p \equiv 3 \pmod 4$, and $a \in \mathbb{Z}_p^*$. Show that the circle $x^2 + y^2 \equiv a \pmod p$ has exactly $p+1$ points (x,y). **(4)**

Solution Consider the two congruences $x^2 \pm y^2 \equiv a \pmod p$ together. Plug in a value $x = h \in \mathbb{Z}_p$. The two congruences now become $y^2 \equiv a - h^2 \pmod p$ and $y^2 \equiv -(a - h^2) \pmod p$. If $a \equiv h^2 \pmod p$, both these congruences have the unique solution $y \equiv 0 \pmod p$. So suppose that $a - h^2 \not\equiv 0 \pmod p$. Since $p \equiv 3 \pmod 4$, we have $\left(\frac{-1}{p}\right) = -1$, that is, exactly one of the two congruences has two roots, and the other has no roots. To sum up, the total number of solutions of the two congruences $x^2 \pm y^2 \equiv a \pmod p$ is $2p$. As in Part (b), we can show that the total number of solutions of $x^2 - y^2 \equiv (x+y)(x-y) \equiv a \pmod p$ is $p-1$.