## **CS60094 Computational Number Theory**

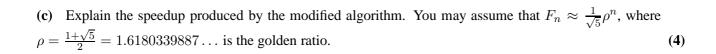
## **Mid-Semester Test**

Maximum marks: 30	February 26, 2010	<b>Duration:</b> 2 hours	
Roll No	Name		

[This test is open-notes. Answer all questions. Be brief and precise.]

- 1 Suppose that  $\gcd(r_0,r_1)$  is computed by the repeated Euclidean division algorithm. Suppose also that  $r_0 > r_1 > 0$ . Let  $r_{i+1}$  denote the remainder obtained by the *i*-th division (that is, in the *i*-th iteration of the Euclidean loop). So the computation proceeds as  $\gcd(r_0,r_1) = \gcd(r_1,r_2) = \gcd(r_2,r_3) = \cdots$  with  $r_0 > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0$  for some  $k \geqslant 1$ .
  - (a) If the computation of  $gcd(r_0, r_1)$  requires exactly k Euclidean divisions, show that  $r_0 \ge F_{k+2}$  and  $r_1 \ge F_{k+1}$ . Here,  $F_n$  is the n-th Fibonacci number:  $F_0 = 0$ ,  $F_1 = 1$ , and  $F_n = F_{n-1} + F_{n-2}$  for  $n \ge 2$ . (4)

(b) Modify the Euclidean gcd algorithm slightly so as to ensure that  $r_i \leqslant \frac{1}{2}r_{i-1}$  for  $i \geqslant 2$ . Here,  $r_i$  need not be the remainder  $r_{i-2}$  rem  $r_{i-1}$ .



- **2** Represent  $\mathbb{F}_{64} = \mathbb{F}_{2^6}$  as  $\mathbb{F}_2(\theta)$  with  $\theta^6 + \theta^3 + 1 = 0$ .
  - (a) Find all the conjugates of  $\theta$  (over  $\mathbb{F}_2$  as polynomials in  $\theta$  of degrees < 6). (4)

<b>(b)</b>	Prove or disprove: $\theta$ is a primitive element of $\mathbb{F}_{64}^*$ .	(4)
(2)	What is the minimal polynomial of $\theta^3$ over $\mathbb{F}_2$ ?	(4)
(c)	what is the minimal polynomial of $\theta^*$ over $\mathbb{F}_2$ ?	(4)