

Math 55: Midterm #1, 24 September 1998

Write your name, your student ID number, your section time and number, your GSI's name and a grading grid (see right) on the cover of your blue book. Books, notes, calculators, scratch paper and/or collaboration are not allowed. Remain in your seat and hand in your exam book *to your GSI* promptly at 5:00 pm; solutions will be available after all exams have been collected. If you finish early, check over your work — do not leave early!

1	
2	
3	
4	
Total	

Problem 1 (25 points):

- (a) Use a truth table to show $p \rightarrow q \Leftrightarrow \neg p \vee q$.
- (b) Show by applying logical equivalences that $p \wedge (p \rightarrow q) \rightarrow q$ is a tautology. State which logical equivalence is used at each step.

Problem 2 (25 points):

- (a) Run the Euclidean algorithm to compute $\gcd(32, 7)$.
- (b) Find an inverse d of $7 \pmod{32}$ with $0 \leq d < 32$. Verify your result.
- (c) Use the procedure of the Chinese Remainder Theorem to find an integer x such that $0 \leq x < 51$ and

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 9 \pmod{17}\end{aligned}$$

Verify your result.

- (d) Suppose that for some unknown integer M with $0 \leq M < 51$, RSA encryption with $N = 51$ and $e = 7$ produces a coded message

$$C = M^e \pmod{N} = 2.$$

State Fermat's little Theorem and use it to show that

$$\begin{aligned}M &\equiv 2 \pmod{3} \\M &\equiv 9 \pmod{17}\end{aligned}$$

- (e) Find the secret message M . Verify your result.

Problem 3 (25 points):

 Define $\mathbf{Z}^+ = \{1, 2, 3, \dots\}$ and

$$\mathbf{Q}^+ = \{p/q \mid p \in \mathbf{Z}^+ \wedge q \in \mathbf{Z}^+ \wedge \gcd(p, q) = 1\}.$$

Define $f : \mathbf{Q}^+ \rightarrow \mathbf{Z}^+$ by $f(p/q) = p + q$. Justify your answers to the following questions.

- (a) Is f one-to-one?
- (b) Is f onto?
- (c) Do \mathbf{Z}^+ and \mathbf{Q}^+ have the same cardinality?

Problem 4 (25 points): Define the Fibonacci numbers by

$$f_0 = 0, \quad f_1 = 1, \quad f_{n+1} = f_n + f_{n-1} \text{ for } n \geq 1.$$

The first few are

$$f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, \dots$$

(a) Write each positive integer $n \leq 12$ as a sum of one or more *distinct* Fibonacci numbers. The first few are

$$1 = f_2, \quad 2 = f_3, \quad 3 = f_4, \quad 4 = f_4 + f_2, \quad 5 = f_4 + f_3 = f_5, \dots$$

(b) Given a positive integer n , how is the sequence (b_2, b_3, \dots, b_m) produced by the following procedure related to n ?

procedure $B(n : \text{positive integer})$

$m := 1$

while $f_{m+1} \leq n$

begin

$m := m + 1$

$b_m := 0$

end

while $m \geq 2$

begin

if $f_m \leq n$ **then**

begin

$n := n - f_m$

$b_m := 1$

end

$m := m - 1$

end

(c) What is the worst-case complexity of $B(n)$ in terms of n in big- O notation? You may use the following formula, which we proved in class:

$$f_m = \frac{1}{\sqrt{5}} (\varphi^m - (1 - \varphi)^m)$$

where

$$\varphi = \frac{1}{2} (1 + \sqrt{5}) = 1.618\dots$$

(d) Prove by induction that *every* positive integer n can be written as a sum of one or more *distinct* Fibonacci numbers. (Hint: Choose m so that $f_m \leq n < f_{m+1}$ and let $k = n - f_m$.)