

## Math 55: Sample Midterm 1, 9 December 2009

Write your name, your student ID number, your section time and number, and a three-problem grading grid, on the cover of your blue book. Remain in your seat and hand in your exam book at 3:30 pm. Books, notes, calculators, scratch paper and/or collaboration are not allowed. Justify your computations: correct answers with inadequate explanation may receive partial credit.

**2: (a)** It returns **T** iff the input function  $f$  is a bijection (a one-to-one correspondence) between  $A$  and  $B$ .

**(b)** The worst case is when  $h$  is always equal to 1 after the inner loop, so the outer loop does not terminate early. Then  $G$  requires  $mn$  evaluations of  $f$ , so the worst-case complexity is  $W(m, n) = O(mn)$ .

**3: (a)** Since  $711 \equiv 61 \equiv -4 \pmod{13}$  and  $777 \equiv -3 \pmod{13}$  we have

$$7 \times -2 \times -4 \times -3 \equiv -14 \times 12 \equiv -12 \equiv 1 \pmod{13}.$$

**(b)** Since  $666 \equiv 6 \pmod{11}$ ,  $666^{77} \equiv 6^{77} \pmod{11}$ . The relevant powers of  $6 \pmod{11}$  are  $6^2 = 36 \equiv 3$ ,  $6^4 = 9$ ,  $6^8 = 81 \equiv 4$ ,  $6^{16} = 16 \equiv 5$ ,  $6^{32} = 25 \equiv 3$ ,  $6^{64} = 9$ , and  $77 = 64+8+4+1$  so  $6^{77} \equiv 9 \times 4 \times 9 \times 6 \equiv 3 \times -1 \equiv -3 \equiv 8 \pmod{11}$ . Alternatively,  $6^{77} = (6^7)^{11} \equiv (9 \times 3 \times 6)^{11} \equiv 8^{11} = 2^{33} = 32^6 \times 8 \equiv 8 \pmod{11}$ .

**5: (a)** One, by the Chinese Remainder Theorem, since 7, 8 and 9 are pairwise relatively prime.

**(b)** Plugging into the congruences gives

$$\begin{aligned} 2 \cdot x_1 &\equiv 0 \pmod{7} \\ -1 \cdot x_2 &\equiv 1 \pmod{8} \\ 2 \cdot x_3 &\equiv 2 \pmod{9} \end{aligned}$$

so  $x_1 = 0$ ,  $x_2 = -1$  and  $x_3 = 1$  give a solution. Checking, we get  $x = -7 \equiv 497 \pmod{7 \cdot 8 \cdot 9}$ .

**6:**

**Base:** Clearly  $7|a_0$  and  $7|a_1$  so the cases  $n = 0$  and  $n = 1$  are true. This forms a base because the recurrence requires two previous terms.

**Induction:** Fix  $n > 0$  and assume  $7|a_k$  for  $k < n$ . Then by definition of  $|$ , for each  $k < n$  there is an integer  $b_k$  such that  $a_k = 7b_k$ . Then

$$a_n = 2 \cdot 7 \cdot b_{n-1} + 7 \cdot b_{n-2} = 7 \cdot (2b_{n-1} + b_{n-2}),$$

so  $7|a_n$ .

**7: (a)** The truth table reads

$p$	$q$	$p \rightarrow q$	$\neg p \vee q$
T	T	T	$F \vee T = T$
T	F	F	$F \vee F = F$
F	T	T	$T \vee T = T$
F	F	T	$T \vee F = T$

**(b)**

$p \wedge (p \rightarrow q) \rightarrow q$	
$\Leftrightarrow \neg(p \wedge (\neg p \vee q)) \vee q$	Part (a) twice
$\Leftrightarrow (\neg p \vee \neg(\neg p \vee q)) \vee q$	deMorgan
$\Leftrightarrow (\neg p \vee (p \wedge \neg q)) \vee q$	deMorgan and double negation
$\Leftrightarrow ((\neg p \vee p) \wedge (\neg p \vee \neg q)) \vee q$	Distributive law
$\Leftrightarrow (T \wedge (\neg p \vee \neg q)) \vee q$	Excluded middle
$\Leftrightarrow (\neg p \vee \neg q) \vee q$	Domination
$\Leftrightarrow \neg p \vee \neg q \vee q$	Associativity
$\Leftrightarrow \neg p \vee T$	Excluded middle
$\Leftrightarrow T$	Domination

**8: (a)** Every element  $n$  of  $\mathbf{Z}^+$  is given by  $n = f(p/q)$  for  $p/q = n/1 \in \mathbf{Q}^+$ . Hence  $f$  is onto. (Since  $f(5/3) = f(3/5) = 8$ ,  $f$  is not one-to-one.)

**(b)** Since  $\mathbf{Z}^+$  is  $\mathbf{N}$  with 0 removed, it is infinite and countable. We know that the rationals are countable, and a (bijective image of a) subset of a countable set is countable, so  $\mathbf{Q}^+$  is countable. Since it contains  $\mathbf{Z}^+$ , it is infinite, so  $\mathbf{Z}^+$  and  $\mathbf{Q}^+$  have the same cardinality.

**9: (a)** Running the Euclidean algorithm forward gives

$$32 = 4 \cdot 7 + 4$$

$$\begin{aligned} 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \quad \rightarrow \quad \boxed{\gcd(32, 7) = 1.} \end{aligned}$$

(b) Working backward, we find  $\gcd(32, 7)$  as a linear combination of 32 and 7:

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) \\ &= -1 \cdot 7 + 2 \cdot 4 = -1 \cdot 7 + 2 \cdot (32 - 4 \cdot 7) \\ &= 2 \cdot 32 - 9 \cdot 7. \end{aligned}$$

Taking this mod 32 gives

$$1 \equiv -9 \cdot 7 \equiv 23 \cdot 7 \pmod{32} \quad \rightarrow \quad \boxed{d = 23.}$$

Check:  $7 \cdot 23 = 161 = 5 \cdot 32 + 1 \equiv 1 \pmod{32}$ .

(c) As in the Chinese Remainder Theorem, we seek a solution  $x$  of the form

$$x = x_1 \cdot 17 + x_2 \cdot 3,$$

which yields independent decoupled congruences

$$\begin{aligned} 17x_1 &\equiv 2x_1 \equiv 2 \pmod{3} \\ 3x_2 &\equiv 9 \pmod{17} \end{aligned}$$

for  $x_1$  and  $x_2$ . Since  $\gcd(2, 3) = \gcd(3, 17) = 1$ , both are easy to solve:  $x_1 = 1$  and  $x_2 = 3$ . Putting it all back together,  $\boxed{x = 26}$ . Check:  $x \bmod 3 = 2$  and  $x \bmod 17 = 9$ .

(d) The original message is

$$M = C^d \bmod N.$$

Here  $d$  is the inverse of  $e \pmod{(p-1)(q-1)}$  with  $N = pq$ , which is the inverse of  $7 \pmod{32}$ . From part (b), we know  $d = 23$ , so

$$M = 2^{23} \bmod 51.$$

Fermat's little Theorem says that  $a^{p-1} \equiv 1 \pmod{p}$  if  $p$  is prime and  $\gcd(a, p) = 1$ . In the present case, FLT implies

$$\begin{aligned} 2^2 &\equiv 1 \pmod{3} \\ 2^{16} &\equiv 1 \pmod{17}, \end{aligned}$$

so

$$\begin{aligned}2^{23} &\equiv 2 \pmod{3} \\2^{23} &\equiv 2^7 \equiv (-1) \cdot 2^3 \equiv -8 \equiv 9 \pmod{17},\end{aligned}$$

(e) By parts (c) and (d), we have  $M = 26$ . Check:  $26^7 = 52^3 13^3 26 \equiv 13^4 2 \equiv 16^2 2 \equiv 2 \pmod{51}$ .

10: (a) Since  $f(-8, 13) = f(0, 0) = 0$ ,  $f$  is not 1-1.

(b) However,  $f$  is onto. By the Euclidean algorithm,

$$\begin{array}{r}13 \ 8 \ 5 \\8 \ 5 \ 3 \\5 \ 3 \ 2 \\3 \ 2 \ 1 \\2 \ 1 \ 0\end{array}$$

we see that  $\gcd(13, 8) = 1$ . Working backwards, we find the gcd as a linear combination:

$$\begin{aligned}1 &= 3 - 2 = 3 - (5 - 3) \\&= -1 \cdot 5 + 2 \cdot 3 = -1 \cdot 5 + 2 \cdot (8 - 5) \\&= 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (13 - 8) \\&= -3 \cdot 13 + 5 \cdot 8.\end{aligned}$$

Thus for any  $n \in \mathbf{Z}$  we have

$$n = n \cdot 1 = n \cdot (-3) \cdot 13 + n \cdot 5 \cdot 8 = f(-3n, 5n).$$

(c) For  $n = 4$  we have  $s = -12$  and  $t = 20$ .

(d) Taking both sides of the equation

$$4 = -12 \cdot 13 + 20 \cdot 8$$

mod 13 gives the congruence

$$4 \equiv 20 \cdot 8 \pmod{13}.$$

But  $20 \equiv 7 \pmod{13}$ , so the solution is  $t = 7$ .

**11: (a)** It returns **T** iff the input function  $f$  is a bijection (a one-to-one correspondence) between  $A$  and  $B$ .

**(b)** The worst case is when  $h$  is always equal to 1 after the inner loop, so the outer loop does not terminate early. Then  $G$  requires  $mn$  evaluations of  $f$ , so the worst-case complexity is  $W(m, n) = O(mn)$ .

**12:** Proof by contradiction: Assume  $B$  is countable. Then by the assumption, so is  $A$ . This contradicts the hypothesis, so  $A$  must be uncountable.

**13:** By definition of implication, the given proposition is equivalent to

$$\neg(p \wedge q) \vee (p \vee q).$$

By de Morgan, this is equivalent to

$$(\neg p \vee \neg q) \vee (p \vee q)$$

which by associativity and commutativity is

$$(\neg p \vee p) \vee (\neg q \vee q).$$

By excluded middle, this is  $T \vee T$  which is  $T$  by domination.

**14: (a)** It returns **T** iff the input function  $f$  is a bijection (a one-to-one correspondence) between  $A$  and  $B$ .

**(b)** The worst case is when  $h$  is always equal to 1 after the inner loop, so the outer loop does not terminate early. Then  $G$  requires  $mn$  evaluations of  $f$ , so the worst-case complexity is  $W(m, n) = O(mn)$ .

**17: (a)** Straightforward arithmetic gives

$$1 = f_2, 2 = f_3, 3 = f_4, 4 = f_4 + f_2, 5 = f_4 + f_3 = f_5, 6 = f_5 + f_2,$$

$$7 = f_5 + f_3, 8 = f_5 + f_4 = f_6, 9 = f_6 + f_2, 10 = f_6 + f_3, 11 = f_6 + f_4, 12 = f_6 + f_4 + f_2.$$

**(b)** The sequence is the “digits” of  $n$  in the Fibonacci number system:

$$n = b_2 f_2 + b_3 f_3 + \cdots + b_m f_m$$

where each  $b_i$  is 0 or 1. Thus  $(b_2, \dots, b_m)$  tells us which distinct Fibonacci numbers sum to  $n$ .

(c) The procedure takes exactly  $m$  steps, each at worst costing one subtraction. We know that

$$f_m = \text{nearest integer to } \frac{1}{\sqrt{5}}\varphi^m = O(\varphi^m)$$

where  $\varphi = (1 + \sqrt{5})/2$ , so

$$f_m \leq n < f_{m+1} \quad \rightarrow \quad \varphi^m = O(n) \quad \rightarrow \quad m = O(\log_\varphi n) = O(\log n)$$

and the procedure has worst-case complexity  $\boxed{O(\log n)}$ .

(d) **Base:** From (a), the statement is true for  $n = 1$ .

**Induction:** Suppose it is true for  $1, 2, \dots, n - 1$ . Let's prove it is true for  $n$ . Choose  $m$  so that  $f_m \leq n < f_{m+1}$ , and let  $k = n - f_m$ . Note that  $k < f_{m+1} - f_m = f_{m-1}$ . Since  $k < n$ , the inductive hypothesis implies that  $k$  is a sum of distinct Fibonacci numbers, and since  $k < f_{m-1}$  the Fibonacci numbers which sum to  $k$  must be taken from the set  $\{f_2, f_3, \dots, f_{m-2}\}$ . Hence  $n = k + f_m$  has a representation as a sum of *distinct* Fibonacci numbers.

(e) The representation becomes unique if we require that no two adjacent Fibonacci numbers appear, because  $f_{n+1} = f_n + f_{n-1}$ . Procedurally, we scan any bit string representing  $n$  from left to right, replacing any substring 011 by 100 until no consecutive 1s remain.