

Math 55: Midterm #1, 19 February 1998

**Problem 1:** (10 points) Prove that  $(p \wedge q) \rightarrow (p \vee q)$  is a tautology without using a truth table. Justify each step.

**Solution:** 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

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

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

**Problem 2:** (10 points) Let  $A$  be an uncountable set and  $B$  be another set such that  $A \subset B$ . Prove  $B$  is uncountable.

**Solution:** Proof by contradiction: Assume  $B$  is countable. Then by a homework problem, so is  $A$ , since any subset of a countable set is countable. This contradicts the hypothesis, so  $A$  must be uncountable.

**Problem 3:** (20 points) Let  $\mathbf{Z}$  be the set of integers and define  $f : \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$  by  $f(s, t) = 13s + 8t$ .

- (a) Is  $f$  1-1? Why or why not?
- (b) Is  $f$  onto? Why or why not?
- (c) Find integers  $s$  and  $t$  such that  $4 = 13s + 8t$ .
- (d) Find an integer solution  $t$  of the congruence  $8t \equiv 4 \pmod{13}$  satisfying  $0 \leq t < 13$ .

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

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

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

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  $t = 7$ .

**Problem 4:** (20 points) Consider the following pseudocode:

```
function G(set A = {a1, a2, ..., an}, set B = {b1, b2, ..., bm}, function f : A → B)
  do i := 1, m
    integer h := 0
    do j := 1, n
      if (f(aj) = bi) then h := h + 1
    end do
    if (h ≠ 1) then return F
  end do
  return T
end
```

(a) What function of  $f$ ,  $A$  and  $B$  does  $G$  return?

(b) What is its worst-case complexity  $W(m, n)$  in terms of  $m$  and  $n$  in big- $O$  notation?

**Solution:** (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  $W(m, n) = O(mn)$ .

**Problem 5:** (20 points) (a) Encrypt the message  $M = 3$  in the RSA system with  $p = 2$ ,  $q = 13$  and  $e = 11$ .

(b) Decrypt the encrypted message  $C = 25$  in the same system.

**Solution:** (a) The encrypted message is

$$C = M^e \pmod{26} = 3^{11} \pmod{26} = 9$$

since  $3^3 = 27 \equiv 1 \pmod{26}$ .

(b) To decrypt, we need the inverse of  $e = 11 \pmod{(p-1)(q-1)}$ , in other words mod 12. But  $11 \equiv -1 \pmod{12}$  so 11 is its own inverse mod 12. Thus

$$M = C^d = C^{11} \equiv (-1)^{11} \equiv -1 \equiv 25 \pmod{26}.$$

**Problem 6:** (20 points) Define a sequence  $a_n$  by  $a_0 = 7$ ,  $a_1 = 14$  and  $a_n = 2a_{n-1} + a_{n-2}$  for  $n \geq 2$ . Use strong induction to prove that  $7|a_n$  for  $n \geq 0$ .

**Solution:**

**Base:** Clearly  $7|a_0$  so the case  $n = 0$  is true.

**Induction:** Fix  $n > 0$  and assume  $7|a_k$  for  $k > n$ . Then 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  $7|a_n$ .