

## MATH 145, SAMPLE PROBLEMS FOR EXAM 2, 07 MAR, 2008

(Here is a sampling of problems to help you prepare for Exam 2. In order to get the most out of them, hide the solutions until you have worked the problems yourself.)

- (1) What is  $3^{1024}$  in  $\mathbb{Z}_7$ ?

$$3^{1024} = 9^{512} \equiv_7 2^{512} = 4^{256} = 16^{128} \equiv_7 2^{128} = 16^{32} \equiv_7 2^{32} = 16^8 \equiv_7 2^8 = 16^2 \equiv_7 4.$$

- (2) What is  $23^{36}$  in  $\mathbb{Z}_{37}$ ?

Since 37 is prime and  $36 = 37 - 1$ , Fermat's Little Theorem tells us the answer is 1. (I.e.,  $a^{p-1} \bmod p = 1$ , for  $a \neq 0$  in  $\mathbb{Z}_p$ .)

- (3) In designing a toy RSA encryption system, the public data is  $N = 33$ , with public key  $e = 3$ . Answer the following:

- (a) What is the encryption  $f(8)$  of 8?

$$f(8) = 8^3 \bmod 33 = 17.$$

- (b) What is the private key  $d$ ?

The private key is the multiplicative inverse of 3 in  $\mathbb{Z}_{(3-1)(11-1)} = \mathbb{Z}_{20}$ , namely  $d = 7$ . (Since  $3 \cdot 7 = 21 \equiv_{20} 1$ .)

- (c) Why is  $e = 4$  a bad choice for public key?

4 has no multiplicative inverse in  $\mathbb{Z}_{20} = \mathbb{Z}_{\varphi(33)}$  because 4 and 20 are not relatively prime. This implies that there are distinct  $x$  and  $y$  in  $\mathbb{Z}_{33}$  with  $f(x) = f(y)$ ; i.e., there is no decryption.

- (4) Use truth table semantics to establish the following.

- (a)  $p \Rightarrow (q \Rightarrow p)$  is a tautology.

$p$	$q$	$q \Rightarrow p$	$p \Rightarrow (q \Rightarrow p)$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Since the rightmost column consists only of 1s, we infer that the given expression is true no matter what truth values are given to its atomic subexpressions.

(b)  $p \Rightarrow (p \Rightarrow q)$  is not a tautology.

By assigning the truth value 1 (true) to  $p$  and 0 (false) to  $q$ , the truth value of  $p \Rightarrow q$  is 0; hence so is the truth value of  $p \Rightarrow (p \Rightarrow q)$ . Since this expression can be false, it is not a tautology.

(5) Define the new propositional connective  $*$  by the truth condition

$$T(p * q) = (T(p) \cdot T(q)) + T(q)$$

(addition and multiplication in  $\mathbb{Z}_2$ ). Write down the truth table for  $p * q$ , and find a logically equivalent expression that uses the propositional variables  $p$  and  $q$ , plus—at most—the connectives  $\neg$ ,  $\vee$ , and  $\wedge$ .

The truth condition above yields the following truth table for  $p * q$ :

$p$	$q$	$p * q$
0	0	0
0	1	1
1	0	0
1	1	0

Since  $T(p * q) = (T(p) + 1)T(q)$ , we see that  $p * q$  is logically equivalent to  $\neg p \wedge q$ .

(6) (a) State the converse of the statement, “If it’s Tuesday, then I’m in Belgium.”

“If I’m in Belgium, then it’s Tuesday.”

(b) State the contrapositive of the statement, “If it’s Tuesday, then I’m in Belgium.”

“If I’m not in Belgium, then it’s not Tuesday.”

(7) Show that  $p \Rightarrow (p \vee q)$  is a tautology whose converse is not a tautology.

The truth table for this expression gives all values of 1; hence it is a tautology. However, giving  $p$  the truth value 0 and  $q$  the truth value 1, we obtain the truth value of 0 for the converse  $(p \vee q) \Rightarrow p$ .

(8) Using  $P(x, y, z)$  as a predicate that states, “ $x$  is the product of  $y$  and  $z$ ,” write a formula in the free variable  $x$ , saying that  $x$  is a perfect square.

So our universe  $U$  is the set  $\mathbb{Z}$  of integers; our formula is then

$$\exists y P(x, y, y)$$

- (9) Using  $L(x, y)$  as a predicate that states, “ $x$  is strictly less than  $y$ ,” write a sentence—i.e., a formula with no free variables— that says there is no greatest integer.

Again our universe is the set of integers; our sentence says that, given any integer, there is one that is strictly larger. This translates to

$$\forall x \exists y L(x, y)$$

- (10) If  $R(x, y)$  is a binary predicate interpreted in a universe  $U$ , write a sentence that expresses the fact that  $R$  is a transitive relation.

$$\forall x \forall y \forall z [(R(x, y) \wedge R(y, z)) \Rightarrow R(x, z)]$$

- (11) Imagine a mathematical statement  $S$  having the logical form  $P \Rightarrow Q$ . What would be your strategy if you wanted to:

- (a) Prove  $S$  by contraposition.

Assume  $\neg Q$ ; try to infer  $\neg P$ .

- (b) Prove  $S$  by contradiction.

Assume both  $P$  and  $\neg Q$ ; try to derive a logical contradiction.

- (c) Refute  $S$  directly.

Try to prove that  $P$  can be true while  $Q$  is false.

- (12) Let  $P(n)$  (respectively,  $Q(n)$ ) be the statement  $2n+3 < n^2$  (respectively,  $2n+3 \leq n^2$ ), as  $n$  ranges over the nonnegative integers,  $\{0, 1, \dots\}$ .

- (a) Formulate a conjecture about the set  $\{n : P(n) \text{ holds}\}$ .

The statement is false for  $n = 0, 1, 2, 3$ , but seems to be true for  $n = 4$  and higher. So our conjectured truth set is  $\{n : n \geq 4\}$ .

- (b) Formulate a conjecture about the set  $\{n : Q(n) \text{ holds}\}$ .

The statement is false for  $n = 0, 1, 2$ , but seems to be true for  $n = 3$  and higher. So our conjectured truth set is  $\{n : n \geq 3\}$ .

- (c) Use an inductive argument to prove your conjecture about  $P(n)$ .

Based on the conjecture in (a) above, we set  $b = 4$  as our base, and verify that  $11 = 2 \cdot 4 + 3 < 16 = 4^2$ . In the induction step we fix  $n \geq 4$  and hypothesize that  $P(n)$  holds; then we attempt to conclude that  $P(n+1)$  holds. So assume  $2n+3 < n^2$ ; we want to show  $2(n+1)+3 < (n+1)^2$ . Now  $2(n+1)+3 = (2n+3)+2$ , which—by the induction hypothesis—is less than  $n^2+2$ . So it remains to show  $n^2+2 \leq (n+1)^2$ . But this is true just in case  $2 \leq 2n+1$ ; or  $1 \leq 2n$ . Since  $n \geq 4$ , we know  $2n \geq 8$ ; so this is clearly true. (Note: The induction step actually works if we assume  $n \geq 1$ . So why doesn't that prove  $P(n)$  true for  $n \geq 1$ ? Remember: the induction step is a conditional statement, and a conditional statement is always true with a false hypothesis.  $P(n)$  is patently false for  $0 \leq n \leq 3$ .)

- (13) Given the first order linear recurrence:  $T(n) = rT(n-1) + r^n$ ,  $n > 0$ ,  $T(0) = a$  ( $r$  and  $a$  fixed constants).

- (a) Using iteration, formulate a conjecture as to the solution of this recurrence.

We have:  $T(1) = rT(0) + r^1 = ra + r$ ,  $T(2) = rT(1) + r^2 = r^2a + 2r^2$ ,  $T(3) = rT(2) + r^3 = r^3a + 3r^3$ ,  $T(4) = rT(3) + r^4 = r^4a + 4r^4$ . A good guess is that  $S(n) = r^n(a+n)$  is the solution.

- (b) Prove that your conjectured solution is an actual solution.

This uses induction. Taking as base case  $b = 0$ , we verify that  $S(0) = r^0(a+0)$  is actually the given value of  $T(0) = a$ —which it clearly is. Thus  $S(0) = T(0)$ . Next, fix  $n \geq 0$  and assume  $S(n-1) = T(n-1)$ . We need to show  $S(n) = T(n)$ . Indeed,  $T(n) = rT(n-1) + r^n =$  (by the induction hypothesis)  $= rS(n-1) + r^n = r(r^{n-1}(a+(n-1))) + r^n = r^n(a+(n-1)) + r^n = r^n(a+(n-1)+1) = r^n(a+n) = S(n)$ .