

QUIZ 5 : MATH 1200 PROBLEMS, CONJECTURES, PROOFS

APRIL 20, 2009

You have 45 minutes to complete the following quiz. You may use any notes or books but please do not use any calculators. Make sure that you write clearly and use complete sentences. If you provide a calculation, explain why that calculation answers the question.

Each of the following expressions below represent a relation on the set of integers. For each of the expressions:

- (a) find an example of values of a and b which are related and
- (b) find an example of values of a and b which are not related.
- (c) Determine if the relation is reflexive and/or symmetric.
- (d) Determine if the relation is transitive. If it is, give short explanation why, if not, give an example where it fails to be transitive.

- (1) a is related to b if $0 \leq a - b$

Hey, this is the same as $b \leq a$!

- (a) 100 is related to 1
- (b) 1 is not related to 100
- (c) reflexive? yes. because $a - a = 0$ symmetric? no. its not, the example shows it isn't
- (d) transitive? Yes. If $a \geq b$ and $b \geq c$ then $a \geq c$. Also if $0 \leq a - b$ and $0 \leq b - c$ then $0 \leq (a - b) + (b - c) = a - c$.

- (2) a is related to b if a divides b or $b < a$.

- (a) 100 is related to 1
- (b) 5 is not related to 7
- (c) reflexive? yes because a always divides a symmetric? No. for example 7 is related to 5 but 5 is not related to 7
- (d) transitive? no. 3 divides 9 so 3 is related to 9, $8 < 9$ so 9 is related to 8, but 3 is not related to 8 because 8 is not less than 3 and 3 does not divide 8.

- (3) a is related to b if $a \equiv -b \pmod{6}$ or $a \equiv b \pmod{6}$.

This is the same as $a + b$ is divisible by 6 or $a - b$ is divisible by 6.

- (a) 0 is related to 6
- (b) 0 is not related to 1
- (c) reflexive? yes. $a - a$ is always divisible by 6 symmetric? yes. if $a - b$ is divisible by 6 then $b - a$ is divisible by 6 and if $a + b$ is divisible by 6
- (d) transitive? yes. if $a \equiv b \pmod{6}$

- (4) Give the contrapositive of the statement: if q divides a , then there is a $k \in \mathbb{Z}$ such that $a = qk$.
 One expression of the contrapositive is “If for all $k \in \mathbb{Z}$ we see $a \neq qk$, then q does not divide a .”
 Alternatively you can say, “If there does not exist a $k \in \mathbb{Z}$ such that $a = qk$, then q does not divide a .”

- (5) Give the contrapositive of the statement: if $a = k^2$ for some $k \in \mathbb{Z}$, then for all positive integers n , $a \equiv 1 \pmod{n}$.
 “If there is an $n \in \mathbb{N}$, $a \not\equiv 1 \pmod{n}$, then for all $k \in \mathbb{Z}$, $a \neq k^2$.”

- (6) Prove or provide a counterexample: If $a, b \in \mathbb{Z}$ and $n, k \in \mathbb{N}$, such that $a^k \equiv b^k \pmod{n}$, then $a \equiv b \pmod{n}$.

This statement is false. The first counterexample that we would encounter is $n = 3$ and $a = 1$ and $b = -1$ and $k = 2$. $(1)^2 \equiv (-1)^2 \pmod{3}$, but 1 is not equivalent to $-1 \pmod{3}$.

- (7) Prove or provide a counterexample: If $a, b \in \mathbb{Z}$ and $n, k \in \mathbb{N}$, such that $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

This statement is true. We shall justify it by induction. We have that the base case is true for $k = 1$ that if $a \equiv b \pmod{n}$ then clearly $a^1 \equiv b^1 \pmod{n}$.

Now assume that for some fixed k , if $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$. Recall by the homework assignment we showed that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$. Therefore $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$, then $a^{k+1} = a \cdot a^k \equiv b \cdot b^k = b^{k+1} \pmod{n}$ so the statement if $a \equiv b \pmod{n}$, then $a^{k+1} \equiv b^{k+1} \pmod{n}$ is true. By the principle of mathematical induction we have that if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbb{N}$.