KEY

MATH 325K QUIZ.

This quiz consists of 5 questions. Generous partial credit will be awarded. Good luck!

(1) (10 points.) Use mathematical induction to prove that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

for all natural numbers n.

(1) First we check that the statement is true when $n = 1$:

(1) $1^3 = 1 \qquad \left(\frac{1(1+1)}{2}\right)^2 = 1^2 = 1$ So the claim holds for $n=1$.

(1) Now assume the claim holds for $n = k$; that is, assume that

(1) $$1^3 + 2^3 + \cdots + k^3 = \left(\frac{k(k+1)}{2}\right)^2.$$

(1) We shall prove that the claim holds for $n = k+1$; that is,

$$1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = \left(\frac{(k+1)((k+1)+1)}{2}\right)^2.$$

Observe that

(1) $$1^3 + 2^3 + \cdots + k^3 + (k+1)^3 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \quad \text{(induction hyp.)}$$

$$= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4}$$

$$= \frac{k^2(k+1)^2 + 4(k+1)(k+1)^2}{4}$$

$\rightarrow$

(2) (10 points.) Let m and n be odd integers. Prove that 8 divides $m^2 - n^2$.

Since m and n are odd, we may write

(2) $m = 2j+1$ and $n = 2k+1$ for some integers j, k.

(1) So we have $m^2 - n^2 = (2j+1)^2 - (2k+1)^2$

$$= 4j^2 + 4j + 1 - 4k^2 - 4k - 1.$$

$$= 4(j^2 + j - k^2 - k).$$

(2) $$= 4(j(j+1) - k(k+1)). \longrightarrow$$

(3) (15 points.) Let m and n be positive integers greater than 1. Show that there are distinct primes $p_1, \ldots, p_k$ and *non-negative* (i.e. ≥ 0) integers $a_1, \ldots, a_k, b_1, \ldots, b_k$ such that

$$m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}.$$

Also prove that $\gcd(m, n) = p_1^{c_1} \ldots p_k^{c_k}$ where c_i =minimum$(a_i, b_i), 1 \leq i \leq k$.

Since ~~an integer~~ a positive integer cannot be divisible by

(1) any integers greater than itself, each of m and n is

divisible by only finitely many primes. So let

(2) $\{p_1, \ldots, p_k\}$ be the set of primes that divide at

least one of m and n. Then the prime factorization

of each of m and n contains only primes in this set.

(1) Since we can include the 0^{th} power of a prime

$p_j^0 = 1$ in a factorization without changing its

value, we may now write $\longrightarrow$

(4) (15 points.) Let $p(x, y)$ denote a polynomial in two variables with integer coefficients. For instance, $p(x, y) = x^2 - 4y^2 - 2$. Prove that if the equation $p(x, y) = 0$ has an integer solution, then the congruences $p(x, y) \equiv 0 \pmod{n}$ have integer solutions for all n.
Use this to show that the equation $x^2 - 4y^2 = 2$ has no integer solutions.

Suppose that the equation $p(x, y) = 0$ has an integer
solution; that is, there exist integers x_0, y_0 such that
(1) $p(x_0, y_0) = 0$. Then ~~since~~ for each natural number n,
(2) we have $n \mid 0$, and thus $n \mid (p(x_0, y_0) - 0)$. So
(1) $p(x_0, y_0) \equiv 0 \pmod{n}$, and thus (x_0, y_0) is an
(1) integer solution to the congruence $p(x, y) \equiv 0 \pmod{n}$
for every $n \in \mathbb{N}$.

To show that the equation $x^2 - 4y^2 - 2 = 0$ has no
(2) integer solutions, we will find a value of n for which
the congruence $x^2 - 4y^2 - 2 \equiv 0 \pmod{n}$ has no
integer solutions.

(2) Let's try $n = 4$. Notice that $x^2 - 4y^2 - 2 \equiv x^2 - 2 \pmod{4}$
(1) for all integers x, y, since $4y^2$ is a multiple of 4.
So it suffices to show that the congruence $x^2 - 2 \equiv 0$
$\pmod{4}$ has no integer solutions. We will do this by checking
the values in the complete residue set $\{0, 1, 2, 3\}$.

$\longrightarrow$

(5) (10 points.) Calculate the remainder when 6^{48} is divided by 13.

(2) The given task is equivalent to finding an integer r in the complete residue set $\{0, 1, \ldots, 12\}$ such that $6^{48} \equiv r \pmod{13}$.

(1) By Fermat's Little Theorem, since 13 is prime, and $(6, 13) = 1$ we have

(1) (2) $$6^{12} \equiv 1 \pmod{13}.$$

So we see that

$$
\begin{aligned}
6^{48} &= (6^{12})^4 && (1)\\
&\equiv 1^4 \pmod{13} && \text{(by 4.4)}\\
&\equiv 1 \pmod{13}. && (2)
\end{aligned}
$$

So $6^{48} \equiv 1 \pmod{13}$; that is, there exists some integer q such that $6^{48} = 13q + 1$.

(1) So the remainder is 1.