Dr. Marques Sophie
Office 519
Number theory
Fall Semester 2014
marques@cims.nyu.edu

MIDTERM

Maximal Score: 200 points

Problem 1: ($\star$) 50 points Find the remainder when 2^{33} is divided by 31.

Solution:
By Fermat's Little Theorem, $2^{31} \equiv 2 \ mod \ 31$. Thus $2^{33} \equiv 8 \ mod \ 31$.

Problem 2: ($\star\star$) 40 points Suppose that $n^2 = \sum_{d|n} f(d)$. Evaluate $f(8)$.

Solution:
By Mobius-inversion formula, $f(n) = \sum_{d|n} \mu(d)(n/d)^2$.

$$f(8) = \sum_{d|8} \mu(d)(8/d)^2 = \mu(1)8^2 + \mu(2)4^2 = 8^2 - 4^2 = 48$$

Problem 3: ($\star$) 10 points
Prove that $n-1$ and $2n-1$ are relatively prime, for all integers $n > 1$.

Solution:
Since $(1)(2n-1) + (-2)(n-1) = 1$, we have $gcd(2n-1, n-1) = 1$. Similarly, $(2)(3n-1) + (-3)(2n-1) = 1$, and so $gcd(3n-1, 2n-1) = 1$.

Problem 4: ($\star$) 15 points
Find all solutions to the congruence $x^2 \equiv p \ mod \ p^2$ when p is a prime number. (Hint: consider mod p).

Solution:
There are no solutions. Indeed, if x satisfies the congruence, then $x^2 \equiv 0 mod p$. Thus p divides x^2, so p divides x and thus p^2 divides x^2. Since we then have $x^2 \equiv 0 \ mod \ p^2$, we do not have $x^2 \equiv p \ mod \ p^2$.

Problem 5: ($\star$) 50 points
Show that n^4+n^2+1 is composite for all $n \geq 2$. (Hint: $n^4+n^2+1 = (n^4+2n^2+1)-n^2$.)
Solution:
If you calculate two or three of these numbers, you see that they are composite but are not systematically divisible by any particular number. This suggests an algebraic factorization. The point turns out to be that $n^4 + n^2 + 1 = (n^4 + 2n^2 + 1) - n^2$ is a difference of two

squares. It's thus the product $(n^2+1+n)(n^2+1-n)$. To prove that this is a non-trivial factorization, you have to see that n^2-n+1 is bigger than 1 but this is easy.

Problem 6: ($\star\star$) 35 points Give all the solution:

1. Solve the system of congruences $5x \equiv 14 \ (mod\ 17)$ and $3x \equiv 2 \ (mod\ 13)$.
2. Solve the congruences $5x \equiv 2 \ (mod\ 10)$.

Solution:

1. By trial and error, $7\times 5 \equiv 1 \ (mod\ 17)$ and $9\times 3 \equiv 1 \ (mod\ 13)$, so $5x \equiv 14 \ (mod\ 17)$; $35x \equiv 98(mod\ 17)$; $x \equiv 13(mod\ 17)$ and $3x \equiv 2(mod\ 13)$; $27x \equiv 18 \ (mod\ 13)$; $x \equiv 5 \ (mod\ 13)$. Having reduced the system to the standard form, we can solve it in the usual way. We have $x = 13+17q$ for some $q \in \mathbb{Z}$, and then $13+17q \equiv 5 \ (mod\ 13)$. This reduces to $4q \equiv 5(mod\ 13)$, so $40q \equiv 50 \ (mod\ 13)$, or $q \equiv 11 \ (mod\ 13)$. This leads to the answer, $x \equiv 13+17\times 11 \equiv 200 \ (mod\ 221)$.
2. No solution.

Problem 7: ($\star\star$) 35 points Prove that $10^{n+1}+4\times 10^n+4$ is divisible by 9, for all positive integers n (Hint: Think!)
Solution:
The proof consists of simply observing that $10^{n+1}+4\times 10^n+4 \equiv 0 \ (mod\ 9)$ since $10 \equiv 1 \ (mod\ 9)$.