

Math 312: Problem set 3 (due 25/5/11)

Calculation

- (Dec 2010 final exam) Let $n = 3^{100}$ and let a be the $2n$ -digit number $858585\dots 8585$ where the digits 85 repeat n times. Is a divisible by 9? Prove your answer.
- (Dec 2005 final exam)
 - Show that $3^6 \equiv 1 \pmod{7}$
Hint: Calculate 3^2 or $3^3 \pmod{7}$ first.
 - Let $a \equiv b \pmod{6}$. Show that $3^a \equiv 3^b \pmod{7}$.
Hint: What can you say about $3^{|a-b|}$? Problem 8 may be useful.
 - Today is Thursday. What day will it be $10^{200,000,000,000}$ days from now?
- (§4.1.E20) Find the least non-negative residue mod 13 of the following numbers: 22, -100 , 1001.
- (squares mod small numbers)
 - For each $m = 3, 4$ find all residues $0 \leq a < m$ which are square mod m (in other words for which there is an integer solution to $x^2 \equiv a \pmod{m}$).
Hint: Let x range over the residues mod m and see what values of a you get.
 - Find an integer x such that $x^2 \equiv -1 \pmod{5}$.
- Find all solutions to: $15x \equiv 9 \pmod{25}$, $2x + 4y \equiv 6 \pmod{8}$.
- (CRT)
 - (§4.3.E10) Find an integer that leaves a remainder of 9 when divided by 10 or 11 but is divisible by 13.
 - (§4.3.E12) If eggs are removed from a basket 2, 3, 4, 5, 6 at a time, 1, 2, 3, 4, 5 eggs remain, respectively. If eggs are removed 7 at a time, no eggs remain. What is the least possible number of eggs in the basket?
Hint: Note that -1 satisfies the congruence conditions mod 2, 3, 4, 5, 6 hence mod their LCM.

Problems

- Powers and irrationals
 - Let $n = \prod_p p^{e_p}$ be the prime factorization of a positive integer and let $k \geq 2$. Show that in the prime factorization of n^k every exponent is divisible by k . Conversely, let $m = \prod_p p^{f_p}$ where $k | f_p$ for all p . Show that m is the k th power of a positive integer.
 - Show that $\sqrt{2}$ is not an integer, that is that there is no integer solution to $x^2 = 2$.
Hint: What is the exponent of 2 in the prime factorization of 2? What do you know about the exponent of 2 in the prime factorization of x^2 ?
 - Show that $\sqrt{2}$ is not a rational number, that is that there are no positive integers x, y such that $\left(\frac{x}{y}\right)^2 = 2$.
Hint: Consider the exponent of 2 on both sides of $x^2 = 2y^2$.
- SUPP Show that $\sqrt{2} + \sqrt{3}$ is irrational.
Hint: Squaring shows that if this number is irrational then so is $\sqrt{6}$.

8. Let $a \equiv b(m)$. Show that $a^n \equiv b^n(m)$ for all $n \geq 0$.
9. Consider the numbers $2^x \pmod 3$ and $3^y \pmod 4$.
- (a) Let $2^x + 3^y = z^2$ for some integers $x, y, z \geq 0$ where $x, y \geq 1$. Show that $(-1)^x \equiv z^2(3)$.
- (b) Use problem 4 to show that $(-1)^x \equiv z^2(3)$ forces x to be even.
Hint: Is (-1) a square mod 3?
- (c) Now show that $(-1)^y \equiv z^2(4)$.
- (d) Finally, show that this forces y to be even.
10. For $n = \sum_{j=0}^J 10^j a_j$ set $T(n) = \sum_{j=0}^J (-1)^j a_j$ (i.e. add the even digits and subtract the odd digits).
- (a) Show that $T(n) \equiv n(11)$.
- (b) Is the number from problem 1 divisible by 11? Justify your answer.
11. (Gaps between squarefree numbers)
- (a) Let $\{p_j\}_{j=1}^J$ be distinct primes. Show that there exist positive integers x such that $p_j^2 | x + j$.
Hint: Rewrite the condition as a congruence condition on x and apply the CRT.
- (*b) Call a number “squarefree” if it is not divisible by the square of a prime (15 is squarefree but 45 isn't). Show that there are arbitrarily large gaps between squarefree numbers.

Supplementary problems (not for submission)

- A. Show that every non-zero rational number can be uniquely written in the form $\varepsilon \prod_p p^{e_p}$ where $\varepsilon \in \{\pm 1\}$, $e_p \in \mathbb{Z}$ and $\{p \mid e_p \neq 0\}$ is finite. Show that a rational number is a k th power iff ε is a k th power and $k | e_p$ for all p .
- B. (The p -adic norm) For a rational number $a = \varepsilon \prod_p p^{e_p}$ with a factorization as above set $|n|_p = p^{-e_p}$ (and $|0|_p = 0$).
- (a) Show that $|a + b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$ and $|ab|_p = |a|_p |b|_p$.
- (b) Show that $d_p(a, b)$