Lior Silberman's Math 312: Problem Set 3 (due 31/5/11)

Calculation

1. (Dec 2005 final exam)
   (a) Show that $3^6 \equiv 1\,(7)$
   Hint: Calculate 3^2 or 3^3 mod 7 first.
   (b) Let $a \equiv b\,(6)$. Show that $3^a \equiv 3^b\,(7)$.
   Hint: What can you say about $3^{|a-b|}$? Problem 8 may be useful.
   (c) Today is Thursday. What day will it be $10^{200,000,000,000}$ days from now?

2. (squares mod small numbers)
   (a) For each $m = 3,4$ find all residues $0 \le a < m$ which are square mod m (in other words for which there is an integer solution to $x^2 \equiv a\,(m)$).
   Hint: Just try all possible values of x.
   (b) Find an integer x such that $x^2 \equiv -1\,(5)$.

3. Find all solutions to: $15x \equiv 9\,(25)$; also to $2x + 4y \equiv 6\,(8)$.

4. 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 modulu $2,3,4,5,6$ hence mod their LCM.

Problems

5. Powers and irrationals
   (a) Let $n = \prod_p p^{e_p}$ be the prime factorization of a positive integer and let $k \ge 2$. 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 kth power of a positive integer.
   (b) 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?
   (c) 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 rational then so is $\sqrt{6}$...

6. Let $a \equiv b\,(m)$. Show that $a^n \equiv b^n\,(m)$ for all $n \ge 0$.

7. Consider the numbers 2^x mod 3 and 3^y mod 4.
   (a) Let $2^x + 3^y = z^2$ for some integers $x,y,z \ge 0$ where $x,y \ge 1$. Show that $(-1)^x \equiv z^2\,(3)$.
   (b) Use problem 2 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.

8. 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.

9. (Gaps between squarefree numbers)
   (a) Let $\left\{p_j\right\}_{j=1}^{J}$ be distinct primes. Show that there exist positive integers x such that for all $1 \leq j \leq J$, $p_j^2 | x+j$.
   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 $\left\{p \mid e_p \neq 0\right\}$ is finite. Show that a rational number is a kth power iff ε is a kth 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 $|a+b|_p \leq \max\left\{|a|_p, |b|_p\right\} \leq |a|_p + |b|_p$ and $|ab|_p = |a|_p |b|_p$.
   (b) Define a "distance" between rational numbers by $d(a,b) = |a-b|_p$ (analogous to the distance defined using the usual absolute value). Show that this new distance satisfies the *triangle inequality*: for all $a, b, c \in \mathbb{Q}$,

$$d(a,c) \leq d(a,b) + d(b,c)\,.$$

   RMK: The p-adic distance encodes congruence information through analysis, a powerful idea due to Kurt Hensel.