M403 Homework 7

Enrique Areyan
October 17, 2012

(1.77) (i) **True**. This is a restatement of Corollary 1.59

(ii) **False**. Let $a = 1, b = 5$ and $m = 4$. Then $(1+5)^4 = 6^4 = 1296 \equiv 0 \bmod 4$, and $1^4+5^4 = 1+625 = 626 \equiv 2 \bmod 4$

(v) **False**. Using the fact that if $a \equiv b \bmod m$ then $a^n \equiv b^n \bmod m$, we can verify this with modulo 10:

$a =$	0	1	2	3	4	5	6	7	8	9
mod 10 $a^2 =$	0	1	4	9	6	5	6	9	4	1

We can write $5263980007 = 526398000 \cdot 10 + 7 \iff 5263980007 \equiv 7 \bmod 10$, but 7 is not a remainder of a square mod 10. Hence, 5263980007 is not a perfect square.

(vi) **False**. Suppose to the contrary that there exists an integer n such that $n \equiv 1 \bmod 100$ and $n \equiv 4 \bmod 1000$. Then,

$$100|n-1 \iff n-1 = 100 \cdot k \iff n = 100 \cdot k + 1, \text{ for some } k \in \mathbb{Z} \text{ and}$$

$1000|n-4 \iff n-4 = 1000 \cdot k' \iff n = 1000 \cdot k' + 4$, for some $k' \in \mathbb{Z} \iff n = 100 \cdot k'' + 4$ where $k'' = 10 \cdot k'$

Contradicting the Division Algorithm, since dividing n by 100 leaves two different remainder according to the two previous equations. Therefore, there exists no such integer n.

(1.79) Let $m \in \mathbb{Z}^+$. Define m' to be a number obtained by rearranging the digits of m. Is $m - m'$ is a multiple of 9?.
Proof: Let d_i denote the ith digit of m and d'_i the ith digit of m'. We can write both m and m' in decimal notation:

$$m = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

$$m' = d'_n \cdot 10^n + d'_{n-1} \cdot 10^{n-1} + \cdots + d'_2 \cdot 10^2 + d'_1 \cdot 10^1 + d'_0 \cdot 10^0$$

Subtracting m' from m:

$$m-m' = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0 - d'_n \cdot 10^n - d'_{n-1} \cdot 10^{n-1} - \cdots - d'_2 \cdot 10^2 - d'_1 \cdot 10^1 - d'_0 \cdot 10^0$$

In the very first homework of the semester we prove that $10^n = 9 \cdot p + 1 \iff 10^n \equiv 1 \bmod 9$, for any n. Also, since $d_i = d'_j$ for some j, we can group the same digits from m and m' to obtain:

$$m - m' \equiv \sum_{i=1}^{n} d_i(1-1) \bmod 9 = \sum_{i=1}^{n} d_i \cdot 0 = \sum_{i=1}^{n} 0 = 0 \Rightarrow m - m' \equiv 0 \bmod 9$$

Which means that $9|m - m' - 0 \iff 9|m - m' \iff m - m' = 9 \cdot k$ for some $k \in \mathbb{Z}$. Q.E.D.

(1.80) Let n be a positive integer and $n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$ be n's decimal notation.

($\Rightarrow$) Suppose that $11|n \iff n = 11 \cdot p$ for some $p \in \mathbb{Z}$. By definition

$$11 \cdot p = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

Since the powers of 10 are congruent to -1 or 1 mod 11 alternatively, we can write (also, rearranging terms):

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0 \equiv d_0(1) + d_1(-1) + \cdots + (-1)^k d_k \bmod 11$$

Hence, $11 \cdot p \equiv d_0 - d_1 + \cdots + (-1)^k d_k \bmod 11$. Call $S = d_0 - d_1 + \cdots + (-1)^k d_k$. Then:

$$11|S - 11 \cdot p \iff S - 11 \cdot p = 11 \cdot q \text{ for some } q \in \mathbb{Z} \iff S = 11 \cdot q + 11 \cdot p = 11(q+p) \iff 11|S$$

($\Leftarrow$) Suppose that $11|S$. Then

$$11|S \iff S = 11 \cdot p \iff 11 \cdot p = d_0 - d_1 + \cdots + (-1)^k d_k \equiv d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0 \bmod 11 = n$$

Hence, $11 \cdot p \equiv n \bmod 11 \iff 11|11 \cdot p - n \iff 11 \cdot p - n = 11 \cdot q \iff n = 11 \cdot p - 11 \cdot q = 11(p-q) \iff 11|n$ Q.E.D.

(1.85) Prove that there are no integers x, y and z such that $x^2 + y^2 + z^2 = 999$.

Proof. If a is a perfect square, then, $a^2 \equiv 0, 1,$ or 4 mod 8. Since $999 = 8 \cdot 124 + 7 \Rightarrow 999 \equiv 7$ mod 8. By proposition 1.60 (i), we have that:

$$x^2 \equiv 0, 1, \text{ or } 4 \text{ mod } 8$$
$$y^2 \equiv 0, 1, \text{ or } 4 \text{ mod } 8$$
$$z^2 \equiv 0, 1, \text{ or } 4 \text{ mod } 8$$

Then the sum is going to be preserve moulo 8. This means that:

$$\begin{aligned}
x^2 + y^2 + z^2 &\equiv 0 \text{ mod } 8 \iff (0+0+0), (4+4+0), (4+0+4), (0+4+4) \\
&\equiv 1 \text{ mod } 8 \iff (1+0+0), (0+1+0), (0+0+1) \\
&\equiv 2 \text{ mod } 8 \iff (1+1+0), (0+1+1), (1+0+1) \\
&\equiv 3 \text{ mod } 8 \iff (1+1+1) \\
&\equiv 4 \text{ mod } 8 \iff (4+0+0), (0+4+0), (0+0+4), (4+4+4) \\
&\equiv 5 \text{ mod } 8 \iff (1+4+0), (0+1+4), (1+0+4), (4+1+0), (0+4+1), (4+1+0) \\
&\equiv 6 \text{ mod } 8 \iff (4+1+1), (1+4+1), (1+1+4) \\
&\equiv 9 \text{ mod } 8 \iff (4+4+1), (4+1+4), (1+4+4)
\end{aligned}$$

All $3^3 = 27$ possibilities are represented above but none of these are $\equiv 7$ mod 8. Hence, there exists no integers x, y, z such that $x^2 + y^2 + z^2 = 999$.

(1.86) Prove that there is no perfect square whose two last digits are 35.

A first proof: if $a \equiv 5$ mod 10 then $a^2 \equiv 5$ mod 10.In particular, this means that the only way a square a^2 ends in 5 is that a also ends in 5. Let $a = 10 \cdot k + 5$. Square it: $a^2 = 100 \cdot k^2 + 100 \cdot k + 25 = 100(k^2 + k) + 25 \iff a^2 \equiv 25$ mod 100. Hence, the last two digits of a^2 are 25 and never 35.
A second proof: the following are all the equivalence classes mod 100 for i^2, where $i = 0, 1, ..., 100$ [1, 4, 9, 16, 25, 36, 49, 64, 81, 0, 21, 44, 69, 96, 25, 56, 89, 24,61, 0, 41, 84, 29, 76, 25, 76, 29, 84, 41, 0, 61, 24, 89, 56, 25, 96, 69, 44, 21, 0, 81, 64, 49, 36, 25, 16, 9, 4, 1, 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 0, 21, 44, 69, 96, 25, 56, 89, 24, 61, 0, 41, 84, 29, 76, 25, 76, 29, 84, 41, 0, 61, 24, 89, 56, 25, 96, 69, 44, 21, 0, 81, 64, 49, 36, 25, 16, 9, 4, 1, 0]
None of these is 35, hence there is no square whose two last digits are 35.

(1.87) If x is an odd number not divisible by 3, prove that $x^2 \equiv 1$ mod 24.

Proof: let $x \in \mathbb{Z}$ be an odd number not divisible by 3. Then, there exists a unique $r \in \{0, 1, ..., 23\}$ such that $x \equiv r$ mod 24, i.e., $x - r = 24 \cdot k \iff x = 24 \cdot k + r$ for some $k \in \mathbb{Z}$. Note that since 24 is divisible by 2, $2|x \iff 2|r$, and since 24 is divisible by 3, $3|x \iff 3|r$. Also, if $x \equiv r$ mod 24 then $x^2 \equiv r^2$ mod 24, so by all this, it suffices to look at odd r not divisible by 3 in $\{0, 1, ..., 23\}$, and look at r^2 mod 24 for such r. The following table summarizes the data:

$x =$	1	5	7	11	13	17	19	23
$x^2 =$	1	25	49	121	169	289	361	529
$x^2 \equiv$ mod 24	1	1	1	1	1	1	1	1

(1.94) (i) Let $S(n) : (a+b)^n \equiv a^n + b^n$ mod 2 for all a, b and for all $n \geq 1$.
Proof that $S(n)$ is true for all $n \geq 1$, by 2nd form of induction.
Base Cases: $n = 1 \Rightarrow (a+b)^1 = a + b \Rightarrow S(1)$ is true. Also, $n = 2 \Rightarrow (a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2$ mod 2, since $2|2ab$. Finally, $n = 3 \Rightarrow (a+b)^3 = a^3 + b^3 + 3ab^2 + 3a^2b = a^3 + b^3 + 3ab(b+a) \equiv a^3 + b^3$ mod 2, by analyzing parity of the term $3ab(b+a)$, we find that is its always the case that $3ab(b+a) \equiv 0$ mod 2 (See (*))
Inductive Step: Assume $S(k)$ is true for $k < n$. Then:

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} && \text{Exponent rule} \\
&\equiv (a+b)(a^{n-1} + b^{n-1}) \text{ mod } 2 && \text{Inductive Hypothesis} \\
&= a^n + ab^{n-1} + a^{n-1}b + b^n && \text{Distributing} \\
&= (a^n + b^n) + ab(a^{n-2} + b^{n-2}) && \text{Grouping} \\
&= (a^n + b^n) + ab(a+b)^{n-2} && \text{IH} \\
&\equiv a^n + b^n \text{ mod } 2 && \text{By analyzing each case as follow (*):}
\end{aligned}$$

(*) If a is even and b is odd (or vice versa), then $a \cdot b \equiv 0$ mod 2. If both a and b are even OR both a and b are odd, then $ab(a+b)^{n-2} = ab(a+b)(a+b)^{n-3} \equiv 0$ mod 2 since $a + b$ is even. Q.E.D

(ii) Let $a = 1$ and $b = 1$. Then $(1+1)^2 = 2^2 = 4 \equiv 1$ mod 3. But $1^2 + 1^2 = 1 + 1 = 2 \equiv 2$ mod 3. Hence, $(a+b)^2 \not\equiv a^2 + b^2$ mod 3