Math 223 Number Theory, Spring '07
Homework 4 Solutions

(1) Prove that all powers in the prime factorization of an integer n are even if and only if n is a perfect square.

Solution: Let n have prime factorization

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$$

If all a_i are even, then

$$n = p_1^{2b_1} p_2^{2b_2} p_3^{2b_3} \cdots p_n^{2b_n} = (p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n})^2$$

where $b_i = a_i/2$ for all i, and so n is a perfect square of an integer $m = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n}$. This argument can be reversed to prove the other direction of the equivalence.

(2) Prove that $30|(n^5 - n)$ for all positive integers n. (Hint: Show that both 5 and 6 divide $n^5 - n$ and then use the fact that if a and b divide a number and $gcd(a, b) = 1$, then ab divides it as well.)

Solution: For $n \in \mathbb{N}$,

$$n^5 - n = n(n^4 - 1) = (n-1)n(n+1)(n^2+1).$$

Now either $n - 1$ or n is divisible by 2 and either $n - 1$, n, or $n + 1$ is divisible by 3. Thus the product $(n - 1)n(n + 1)$ is divisible by $2 \cdot 3 = 6$ and so is $n^5 - n$.

To show $n^5 - n$ is divisible by 5, suppose neither of $n - 1$, n, or $n + 1$ is. Then n must be of the form $5k + 2$ or $5k + 3$ for some $k \in \mathbb{Z}$. If $n = 5k + 2$, then $n^2 + 1 = 25k^2 + 20k + 5$, which is divisible by 5. If $n = 5k + 3$, then $n^2 + 1 = 25k^2 + 30k + 10$, which is also divisible by 5.

Since $n^5 - n$ is divisible both by 5 and 6, and since $gcd(5, 6) = 1$, $n^5 - n$ is divisible by $5 \cdot 6 = 30$.

(3) Prove that the sum of three consecutive cubes is always divisible by 9. (Hint: Let the three consecutive cubes be $(n - 1)^3$, n^3, and $(n + 1)^3$ for some $n \in \mathbb{Z}$.)

Solution: For $n \in \mathbb{Z}$, consider $(n - 1)^3$, n^3, and $(n + 1)^3$. Then

$$(n-1)^3 + n^3 + (n+1)^3 = 3n(n^2 + 2).$$

If n is divisible by 3, then $3n$ is divisible by 9, so we are done. Otherwise, $n = 3k + 1$ or $n = 3k + 2$ for some $k \in \mathbb{Z}$. If $n = 3k + 1$, then $n^2 + 2 = 9k^2 + 6k + 3$, which is divisible by 3. If $n = 3k + 2$, then $n^2 + 2 = 9k^2 + 12k + 6$, which is also divisible by 3. Either way, the product $3n(n^2 + 2)$ is divisible by 9.

(4) (7.5) Define the $\mathbb{M}$-*world* to be the set of positive integers that leave a remainder of 1 when divided by 4. In other words, the only $\mathbb{M}$-numbers that exist are

$$\{1, 5, 9, 13, 17, 21, ...\}.$$

(Another description is that these are the numbers of the form $4t + 1$ for $t = \{0, 1, 2, ...\}$.) In the $\mathbb{M}$-world, we cannot add numbers, but we can multiply them, since if a and b both leave a remainder of 1 when divided by 4 then so does their product. (Do you see why this is true? You are actually proving this in another exercise on this homework.) We say that m $\mathbb{M}$-divides n if $n = mk$ for some $\mathbb{M}$-number k. And we say that n *is an* $\mathbb{M}$-*prime* if its only $\mathbb{M}$-divisors are 1 and itself. (Of course, we don't consider 1 itself to be an $\mathbb{M}$-prime.)

(a) Find the first 6 $\mathbb{M}$-primes.

(b) Find an $\mathbb{M}$-number n that has two *different* factorizations as a product of $\mathbb{M}$-primes.

Solution:

(a) The first 6 $\mathbb{M}$-primes are 5, 9, 13, 17, 21, and 29 (5, 13, 17, and 29 are $\mathbb{M}$-prime because they are prime, and $9 = 3^2$ and $21 = 3 \cdot 7$ are prime because 3 and 7 are not $\mathbb{M}$-numbers).

(b) An example is $441 = 9 \cdot 49 = 21 \cdot 21$.

(5) Determine whether each of the following pairs is congruent modulo 7.

(a) (1,15) (b) (-1,8) (c) (0,42) (d) (-9,5) (e) (-1,699)

Solution:

(a) Yes, since $7|(1-15)$ (b) No, since $7 \not| (-1-8)$ (c) Yes, since $7|(0-42)$ (d) Yes, since $7|(-9-5)$ (e) Yes, since $7|(-1-699)$.

(6) For which positive integers m is each of the following statements true?

(a) $27 \equiv 5 \pmod{m}$ (b) $1000 \equiv 1 \pmod{m}$

Solution:

(a) Equivalently, we are looking for those integers m such that $m|(27-5) = 22$, i.e. we are looking for divisors of 22. They are 1, 2, 11, and 22.

(b) Here we are looking for divisors of 999, which are 1, 3, 9, 27, 37, 111, 333, and 999.

(7) (8.1) Suppose that $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$. Verify that

(a) $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{m}$

Solution:

(a) Since $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, we have that there exist $k, l \in \mathbb{Z}$ such that

$$a_1 - b_1 = km \quad \text{and} \quad a_2 - b_2 = lm.$$

Then adding or subtracting these equations gives

$$(a_1 \pm a_2) - (b_1 \pm b_2) = (k \pm l)m \quad \Longleftrightarrow \quad a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}.$$

(b) Using the notation from (a), we have

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 \\ &= a_2(a_1 - b_1) + b_1(a_2 - b_2) \\ &= a_2 km + b_1 lm \\ &= (a_2 k + b_1 l)m \end{aligned}$$

from which the desired result follows.

(8) Suppose that $ac \equiv bc \pmod{m}$ and that $gcd(c, m) = 1$.

(a) (8.2) Prove that $a \equiv b \pmod{m}$.

(b) Provide a counterexample showing that part (a) is false when the assumption that $gcd(c, m) = 1$ is dropped.

Solution:

(a) By definition, $ac \equiv bc \pmod{m}$ means $m|(ac-bc)$ or $m|c(a-b)$. Thus either $m|c$ or $m|(a-b)$. Since $gcd(c, m) = 1$, it must be that $m|(a-b)$. In other words, it must be that $a \equiv b \pmod{m}$.

(b) For example, $8 \equiv 12 \pmod{4}$ but $4 \not\equiv 6 \pmod{4}$ (here $c = 2$).

(9) (parts of 8.3) Find all incongruent solutions to each of the following congruences.

(a) $7x \equiv 3 \pmod{15}$

(b) $6x \equiv 5 \pmod{15}$

(c) $x^2 \equiv 1 \pmod 8$

Solution:

(a) Since $gcd(7, 15) = 1$ and $1|3$, by Linear Congruence Theorem there is exactly one incongruent solution to $7x \equiv 3 \pmod{15}$. To find it, we first solve the equation $7u + 15v = 1$. By Euclidan Algorithm (or by inspection), it is easy to see that a solution is $(u_0, v_0) = (-2, 1)$. Then $cu_0/g = -6$ (where $c = 3$ and $g = 1$) and so the solution to $7x \equiv 3 \pmod{15}$ is $x \equiv -6 \pmod{15} \equiv 9 \pmod{15}$ (we choose 9 as the representative of the solution set since that is the least residue of x modulo 15).

(b) Here $gcd(6, 15) = 3$ which does not divide 5, so this equation has no solutions.

(c) We have

$$0^2 \not\equiv 1 \pmod 8, \quad 1^2 \equiv 1 \pmod 8, \quad 2^2 \not\equiv 1 \pmod 8, \quad 3^2 \equiv 1 \pmod 8,$$
$$4^2 \not\equiv 1 \pmod 8, \quad 5^2 \equiv 1 \pmod 8, \quad 6^2 \not\equiv 1 \pmod 8, \quad 7^2 \equiv 1 \pmod 8.$$

Thus by inspection, the incongruent solutions to $x^2 \equiv 1 \pmod 8$ are $x = 1, 3, 5,$ and 7.

(10) Prove that the last digit of a perfect square is never 2, 3, 7, or 8. (Hint: Every integer n can be written as $n = 10k + r$ where $k, r \in \mathbb{Z}$ and $0 \leq r < 10$. Then consider $n^2 \pmod{10}$.)

Solution: Given $n \in \mathbb{Z}$, we want to compute the least residue of $n^2 \pmod{10}$ and show it cannot be 2, 3, 7, or 8. Write n as $10k + r$ where $k, r \in \mathbb{Z}$ and $0 \leq r < 10$ (so that r is the last digit of n). Then

$$n^2 = (10k + r)^2 = 100k^2 + 20kr + r^2 \equiv r^2 \pmod{10}.$$

The possible values of $r^2 \pmod{10}$ are

$$0^2 \equiv 0 \pmod{10}, \quad 1^2 \equiv 1 \pmod{10}, \quad 2^2 \equiv 4 \pmod{10}, \quad 3^2 \equiv 9 \pmod{10}, \quad 4^2 \equiv 6 \pmod{10},$$
$$5^2 \equiv 5 \pmod{10}, \quad 6^2 \equiv 6 \pmod{10}, \quad 7^2 \equiv 9 \pmod{10}, \quad 8^2 \equiv 4 \pmod{10}, \quad 9^2 \equiv 1 \pmod{10}.$$

Neither of these values is 2, 3, 7, 8, so n^2 cannot be one of those.