Math 4400 Homework 3
Due: Monday, June 5th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. (10 points) Suppose a and b are nonzero integers. Suppose also that $a \mid b$ and $b \mid a$. Prove (carefully!) that $a = \pm b$.

   Solution: By definition, there exist $c, d \in \mathbb{Z}$ such that $ac = b$ and $bd = a$. But then $acd = a$, which means $cd = 1$. Thus $|c||d| = 1$. But $|c|$ and $|d|$ are integers, so this implies $|c| = 1$ and $|d| = 1$, so $c = \pm 1$ and $d = \pm 1$. In other words, $a = \pm b$.

2. (10 points) Recall that, by definition, we say $a \equiv b \mod n$ if $n \mid (a - b)$. Now, let $x, y, z, n \in \mathbb{Z}$ with $n > 0$. Prove the following facts:
   (a) $x \equiv x \mod n$

   Solution: $x - x = 0$ and every number divides 0. Thus $n \mid (x - x)$, which means $x \equiv x \mod n$

   (b) If $x \equiv y \mod n$, then $y \equiv x \mod n$

   Solution: Since $x \equiv y \mod n$, we know $n \mid (x - y)$. Thus there is some $a \in \mathbb{Z}$ such that $an = x - y$. But then $-an = y - x$, which means $n \mid (y - x)$, and so $y \equiv x \mod n$.

   (c) If $x \equiv y \mod n$ and $y \equiv z \mod n$, then $x \equiv z \mod n$.

   Solution: There exist $a, b \in \mathbb{Z}$ such that $an = x - y$ and $bn = y - z$. Then $(a + b)n = x - y + y - z = x - z$, so $x \equiv z \mod n$.

3. (a) (10 points) Suppose that $ac \equiv bc \mod m$ and $\gcd(c, m) = 1$. Show that $a \equiv b \mod m$.

   Solution: Since $\gcd(c, m) = 1$, there is some x such that $cx \cong 1 \mod n$. Then $acx \equiv bcx \mod n$. Since $cx \cong 1 \mod n$, we can replace both instances of "cx" in that congruence with 1. Thus $a \equiv b \mod n$.

   (b) (5 points) Give two examples showing that a is not necessarily equivalent to b above if $\gcd(c, m) \neq 1$.

   Solution: For example, we can choose $m = 12$. Then $3 \cdot 4 \equiv 6 \cdot 4 \mod 12$ even though $3 \not\equiv 6 \mod 12$. Another example: $5 \cdot 1 \equiv 5 \cdot 6 \mod 25$.

4. Find all incongruent solutions to each of the following congruences:
   (a) (3 points) $7x \equiv 3 \mod 15$

   Solution: We do the Euclidean algorithm on 7 and 15:

$$15 = 2 \cdot 7 + 1$$
$$7 = 7 \cdot 1$$

Then $7(-2) \cong 1 \mod 15$, which means $7 \cdot -6 \cong 3 \mod 15$. So $x \cong -6$ is a solution. To simplify, $x \cong 9$ is a solution. Since $\gcd(7,15) = 1$, there's only 1 solution, so we're done.

(b) (3 points) $6x \equiv 5 \mod 15$

Solution: $\gcd(6,15) = 3$, which doesn't divide 5, so there are no solutions

(c) (3 points) $x^2 \equiv 1 \mod 8$

Solution: Suppose x is a solution. Then $x^2 - 1 = n8$ for some n. But then $\gcd(x^2, 8) = \gcd(x^2 - n8, 8) = 1$, we must have $\gcd(x,8) = 1$. So we check all the numbers x with $0 \leq x \leq 7$ and $\gcd(x,8) = 1$:

$$1^2 \cong 1 \mod 8, 3^2 \cong 1 \mod 8, 5^2 \cong 1 \mod 8, 7^2 \cong 1 \mod 8$$

So there are four incongruent solutions, and they are $x \equiv 1 \mod 8$, $x \equiv 3 \mod 8$, $x \equiv 5 \mod 8$, and $x \equiv 7 \mod 8$,

(d) (3 points) $x^2 \equiv 2 \mod 7$

Solution: We just check by hand:

$a \mod 7$	0	1	2	3	4	5	6
$a^2 \mod 7$	0	1	4	2	2	4	1

So $x \cong 3$ and $x \cong 4$ are the two solutions

(e) (3 points) $x^2 + x + 1 \equiv 0 \mod 5$

Solution: We just check by hand:

$a \mod 7$	0	1	2	3	4
$a^2 + a + 1 \mod 7$	1	3	2	3	1

So there's no solution

5. (10 points) Find all incongruent solutions to the following congruence: $(10+x)^{100} - x \equiv 0 \mod 5$

Solution: $(10+x)^{100} - x \equiv x^{100} - x \mod 5$. Further, we can check by hand (or use Fermat's little theorem) to see that $x^4 \equiv 1 \mod 5$ whenever $x \not\equiv 0 \mod 5$. So we break this problem into two cases: if $x \equiv 0 \mod 5$, then $x^{100} - x = 0 - 0 = 0$, so $x \equiv 0 \mod 5$ is one solution. If $x \not\equiv 0 \mod 5$, then by Fermat's littl theorem:

$$x^{100} - x = \left(x^4\right)^{25} - x \equiv 1 - x \mod 5$$

So $x^{100} - x \equiv 0 \mod 5$ if and only if $1 - x \equiv 0 \mod 5$, or in other words $x \equiv 1 \mod 5$. So our two incogruent solutions are $x \equiv 0 \mod 5$ and $x \equiv 1 \mod 5$.

6. (10 points) Let $a \in \mathbb{Z}$. Show that $a^2 - 3$ is not divisible by 4.

Solution: $a^2 - 3$ is disible by 4 if and only if $a^2 \cong 3 \mod 4$. Whether or not this is true just depends on the equivalence class of a modulo 4, so we check:

$a \mod 4$	0	1	2	3
$a^2 \mod 4$	0	1	4	1

Thus a^2 is never congruent to 3 modulo 4.

7. (10 points) Prove that the following "divisibility tests" work:

(a) An integer is divisible by 4 if and only if its last two digits are divisible by 4

Solution: Suppose $n = \sum_{i=0}^{d} n_{d-i} 10^i$, where $0 \leq n_j < 10$ for all j. If $d \leq 2$ the n just has 2 digits,so the problem is trivial. So suppose $d \geq 3$. Then $10^i \cong 0 \mod 4$ whenever $i \geq 2$, since $4 \mid 100$, so

$$n \cong 10n_{d-1} + n_d \mod 4$$

In particular, $n \cong 0 \mod 4$ if and only if $10n_{d-1} + n_d \cong 0 \mod 4$. But the latter number is just the last two digits of n, so we're done.

(b) An integer is divisible by 9 if and only if the sum of its digits is divisible by 9

Solution: Again, suppose $n = \sum_{i=0}^{d} n_{d-i} 10^i$, where $0 \leq n_j < 10$ for all j. Then $10 \cong 1 \mod 9$, so

$$n \cong \sum_{i=0}^{d} n_{d-i} 1^i \cong \sum_{i=0}^{d} n_{d-i} \mod 9$$

In particular, $n \cong 0 \mod 9$ if and only if $\sum_{i=0}^{d} n_{d-i} \cong 0 \mod 9$, as desired.

(c) An integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. (If the digits of n are $n_0 n_1 \ldots n_d$ then the alternating sum of its digits is $n_0 - n_1 + n_2 - \cdots$)

Solution: Again, suppose $n = \sum_{i=0}^{d} n_{d-i} 10^i$, where $0 \leq n_j < 10$ for all j. Then $10 \cong -1 \mod 11$, so

$$n \cong \sum_{i=0}^{d} n_{d-i} (-1)^i \mod 9$$

In particular, $n \cong 0 \mod 9$ if and only if $\sum_{i=0}^{d} n_{d-i} (-1)^i \cong 0 \mod 9$. If d is even, this is the alternating sum $n_0 - n_1 + n_2 - \cdots$. Otherwise, it's $-n_0 + n_1 - n_2 + \cdots$, which is obviously divisible by 9 if and only if the alternating sum is.