Name: Solutions — Caleb McWhorter
MATH 308
Fall 2021
HW 15: Due 11/22

"It is impossible to be a mathematician without being a poet in soul."
–Sofia Kovalevskaya

Problem 1. (10pt) Perform the following computations modulo 3:

(a) $1234 + 2345$

(b) $1784 \cdot 2021$

(c) 1996^{1997}

(d) 2^{2000}

Solution. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Recall that $a \equiv b \mod n$ if and only if $a - b$ is divisibly by n. This happens if and only if $kn = a - b$ for some $k \in \mathbb{Z}$. But then $a = kn + b$. But then given $a \in \mathbb{Z}$, we can choose a $b \in \{0, 1, \ldots, n-1\}$ such that $a \equiv b \mod n$. Use the division algorithm to find $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ such that $a = qn + r$. But then $a - r = qn$ so that $a - r$ is divisible by n. Therefore, $a \equiv r \mod n$. That is, every integer is equivalent to its remainder from the division algorithm modulo n.

(a) Because we have $1234 = 411(3) + 1$ and $2345 = 781(3) + 2$, we know that $1234 \equiv 1 \mod 3$ and $2345 \equiv 2 \mod 3$. But then…

$$(1234 + 2345) \equiv (1 + 2) = 3 = \big(3(1) + 0\big) \equiv 0 \mod 3$$

Alternatively, we have $1234 + 2345 = 3579$ and $3579 = 1193(3) + 0$. But then $(1234 + 2345) = 3579 \equiv 0 \mod 3$.

(b) We have $1784 = 594(3) + 2$ and $2021 = 673(3) + 2$, so that $1784 \equiv 2 \mod 3$ and $2021 \equiv 2 \mod 3$. But then…

$$1784 \cdot 2021 \equiv 2 \cdot 2 = 4 = 1(3) + 1 \equiv 1 \mod 3$$

Alternatively, we have $1784 \cdot 2021 = 3{,}605{,}464$ and $3{,}605{,}464 = 1201821(3) + 1$. Therefore, we have…

$$1784 \cdot 2021 = 3{,}605{,}464 = \big(1201821(3) + 1\big) \equiv 1 \mod 3$$

(c) Observe that we have $1996 = 665(3) + 1$ so that $1996 \equiv 1 \mod 3$. But then…

$$1996^{1997} \equiv 1^{1997} = 1 \mod 3$$

(d) Observe that we have $2 = 3 - 1$. But then $2 \equiv -1 \mod 3$ because $2 + 1 = 3$. But then…

$$2^{2000} \equiv (-1)^{2000} = 1 \mod 3$$

Problem 2. (10pt) Prove that an integer N is divisible by 3 if and only if its the sum of its digits is divisible by 3.

Solution. Let N be an integer. Express N in base-10 as $a_n a_{n-1} \cdots a_1 a_0$, i.e. write $N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + 1a_0$. We know an integer k is divisible by a positive integer n if and only if $k \equiv 0 \bmod n$. Therefore, it suffices to prove that $N \equiv 0 \bmod 3$ if and only if the sum of its digits is divisible by 3. We have $10 = 3(3) + 1$ so that $10 \equiv 1 \bmod 3$. But then...

$$N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + 1a_0 \equiv 1^n a_n + 1^{n-1} a_{n-1} + \cdots + 1a_1 + 1a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0$$

Therefore, $N \equiv 0 \mod 3$ if and only if $a_n + a_{n-1} + \cdots + a_1 + a_0$; that is, N is divisible by 3 if and only if the sum of its digits is divisible by 3.

Problem 3. (10pt) Prove that for all $n, m \in \mathbb{Z}_{\geq 0}$ that $101^n - 77^m$ is divisible by 4.

Solution. We know an integer k is divisible by a positive integer n if and only if $k \equiv 0 \bmod n$. It then suffices to prove that $101^n - 77^m \equiv 0 \bmod 4$ for all $n, m \in \mathbb{Z}_{\geq 0}$. Observe that $101 = 25(4) + 1$ and $77 = 19(4) + 1$, so that $101 \equiv 1 \bmod 4$ and $77 \equiv 1 \bmod 4$. But then...

$$101^n - 77^m \equiv 1^n - 1^m = 1 - 1 = 0 \mod 4$$

Therefore, $101^n - 77^m$ is divisible by 4 for all $n, m \in \mathbb{Z}_{\geq 0}$.[1]

[1] This theory of modularity that we have developed only works for *integers*. The condition that $n, m \in \mathbb{Z}_{\geq 0}$ is to that 101^n and 77^m are integers, respectively.

Problem 4. (10pt) Find the ones digit of 2^{98} and the tens digit of 7^{100}.

Solution. Let N be an integer. Express N in base-10 as $a_n a_{n-1} \cdots a_1 a_0$, i.e. write $N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + 1a_0$. We know the ones digit of N is a_0. But observe $N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + 1a_0 \equiv 0^n a_n + 0^{n-1} a_{n-1} + \cdots + 0a_1 + 1a_0 \equiv a_0 \bmod 10$. But then the ones digit of N is the value of $N \bmod 10$. Similarly, we know for $n \geq 2$, $10^n \equiv 0 \bmod 100$. But then...

$$N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10^2 a_2 + 10a_1 + 1a_0 \equiv 0^n a_n + 0^{n-1} a_{n-1} + \cdots + 0^2 a_2 + 10a_1 + 1a_0 = [a_1 a_0] \mod 100$$

where $[a_1 a_0]$ represents the base-10 number with digits a_1, a_0. We know the tens digit of N is a_1, which can be easily determined from the value of $N \bmod 100$.

Now observe...

$$\begin{aligned} 2^1 &= 2 \equiv 2 \mod 10 & 2^4 &= 2^3 \cdot 2 \equiv 8 \cdot 2 = 16 \equiv 6 \mod 10 \\ 2^2 &= 4 \equiv 4 \mod 10 & 2^5 &= 2^4 \cdot 2 \equiv 6 \cdot 2 = 12 \equiv 2 \mod 10 \\ 2^3 &= 8 \equiv 8 \mod 10 & & \end{aligned}$$

From the work above, it is clear that the value of $2^k \bmod 10$ is cyclic with values $2, 4, 8, 6, 2, 4, 8, 6, \ldots$ beginning at $k = 1$. Therefore, the value of 2^k only depends on the value of 98 modulo 4 (the length of the repeating cycle). We have...

$$2^{98} = 2^{24(4)+2} = 2^{24(4)} \cdot 2^2 = (2^4)^{24} \cdot 2^2 = (2^4)^{6 \cdot 4} \cdot 2^2 \equiv 6 \cdot 4 = 24 \equiv 4 \mod 10$$

Alternatively, observe $2^1 = 2 \bmod 10$, $2^2 = 4 \bmod 10$, $2^4 = (2^2)^2 \equiv 4^2 = 16 \equiv 6 \bmod 10$, $2^8 = (2^4)^2 \equiv 6^2 = 36 \equiv 6 \bmod 10$, $2^{16} = (2^8)^2 \equiv 6^2 = 36 \equiv 6 \bmod 10$, $2^{32} = (2^{16})^2 \equiv 6^2 = 36 \equiv 6 \bmod 10$, and $2^{64} = (2^{32})^2 \equiv 6^2 = 36 \equiv 6 \bmod 10$. But then...

$$2^{98} = 2^{64+32+2} = 2^{64} \cdot 2^{32} \cdot 2^2 \equiv 6 \cdot 6 \cdot 4 = 144 \equiv 4 \mod 10$$

Therefore, the ones digit of 2^{98} is 4.

Now observe...

$$\begin{aligned} 7^1 &= 7 \equiv 7 \mod 100 \\ 7^2 &= 49 \equiv 49 \mod 100 \\ 7^3 &= 343 = 3(100) + 43 \equiv 43 \mod 100 \\ 7^4 &= 7^3 \cdot 7 \equiv 43 \cdot 7 = 301 = 3(100) + 1 \equiv 1 \mod 100 \end{aligned}$$

From the work above, it is clear that $7^{4k} \equiv 1 \bmod 100$ for all integers $k \geq 0$. But $100 = 25(4)$ so that...

$$7^{100} = 7^{25(4)} = (7^4)^{25} = 1^{25} = 1 = [01] \mod 100$$

where $[01]$ is the base-10 integer with the given digits. Therefore, the tens digit of 7^{100} is 0.

Problem 5. (10pt) For the following congruences, find a solution or explains why none exists.

(a) $2x \equiv 3 \mod 7$

(b) $6x \equiv 5 \mod 8$

(c) $4x \equiv 8 \mod 22$

Solution. Let a, b, x be integers, n be a positive integer, and $d = \gcd(a, n)$. Recall that a linear congruence $ax \equiv b \bmod n$ has a solution if and only if d divides b. If $d \mid b$, there are infinitely many solutions and they are all of the form $\frac{sb}{d} + \frac{n}{d} z$, where $z \in \mathbb{Z}$ and s is such that for some y, $d = sx + ny$. When $d = 1$, we can express this simply using the inverse: the solutions modulo n are $x \equiv a^{-1}b$, where a^{-1} is the inverse of a modulo n (which exists because $\gcd(a, n) = 1$). Let s be the integer $1 \le s \le n$ such that $s \equiv a^{-1}b$ modulo n. Then general solutions are $x = s + zn$, where $z \in \mathbb{Z}$.

(a) Observe that $\gcd(2, 7) = 1$ and 3 is divisible by 1. Therefore, there is a solution. We can use inverses to solve this congruence. Observe that $2 \cdot 4 = 8 \equiv 1 \bmod 7$. Therefore, $2^{-1} = 4 \bmod 7$. Then we have...

$$
\begin{aligned}
2x &\equiv 3 \mod 7 \\
2^{-1} \cdot 2x &\equiv 2^{-1} \cdot 3 \mod 7 \\
(2^{-1}2)x &\equiv 4 \cdot 3 \mod 7 \\
1x &\equiv 12 \mod 7 \\
x &\equiv 5 \mod 7
\end{aligned}
$$

Therefore, the solutions are the integers equivalent to 5 modulo 7, i.e. $\ldots, -9, -2, 5, 12, 19, \ldots$.

(b) Observe that $\gcd(6, 8) = 2$ and 5 is not divisible by 2. Therefore, there are no solutions to this congruence. One can verify this by checking all the possible solutions modulo 8

$$
\begin{aligned}
&x \equiv 0 : 6(0) = 0 \not\equiv 5 \mod 8 && x \equiv 4 : 6(4) = 24 \equiv 0 \not\equiv 5 \mod 8 \\
&x \equiv 1 : 6(1) = 6 \not\equiv 5 \mod 8 && x \equiv 5 : 6(5) = 30 \equiv 6 \not\equiv 5 \mod 8 \\
&x \equiv 2 : 6(2) = 12 \equiv 4 \not\equiv 5 \mod 8 && x \equiv 6 : 6(6) = 36 \equiv 4 \not\equiv 5 \mod 8 \\
&x \equiv 3 : 6(3) = 18 \equiv 2 \not\equiv 5 \mod 8 && x \equiv 7 : 6(7) = 42 \equiv 2 \not\equiv 5 \mod 8
\end{aligned}
$$

(c) Observe that $\gcd(4, 22) = 2$ and 8 is divisible by 2. Therefore, there is a solution (infinitely many in fact). However, because $\gcd(4, 22) \neq 1$, we know that 4^{-1} does not exist. Therefore, inverses cannot be used to solve this congruence. But using the comments above, we know the solutions have the form $\frac{xb}{d} + \frac{n}{d} z$, where $z \in \mathbb{Z}$ and x is such that for some y, $d = ax + ny$. Using the Euclidean algorithm, we write $2 = 4(-5) + 22(1)$. So we know $x = -5$. Therefore, the solutions are the integers of the form...

$$\frac{xb}{d} + \frac{n}{d} z = \frac{-5(8)}{2} + \frac{22}{2} z = -20 + 11z = 11z - 20$$

where z is an integer. For example, $-31, -20, -9, 2, 13, 24$ are solutions resulting from the choices $z = -1, 0, 1, 2, 3, 4$, respectively. We can also see this directly:

$$4x \equiv 4(11z - 20) = 44z - 80 = 2(22z) + (-4 \cdot 22 + 8) \equiv 0 + (0 + 8) = 8 \mod 22$$

Problem 6. (10pt) Use the Chinese Remainder Theorem to find the solutions modulo 60 to...

$$\begin{aligned} x &\equiv 3 \mod 4 \\ x &\equiv 2 \mod 3 \\ x &\equiv 4 \mod 5 \end{aligned}$$

Solution. Suppose we have a system of congruences $x \equiv a_1 \bmod n_1$, $x \equiv a_2 \bmod n_2$, ..., $x \equiv a_k \bmod n_k$. The Chinese Remainder Theorem (also known as Sunzi's Theorem), states that if the n_i are pairwise coprime, i.e. $\gcd(n_i, n_j) = 1$ for all i, j with $i \neq j$, there is a solution and this solution is unique modulo $N = n_1 n_2 \cdots n_k$. Furthermore, the theorem states that the solution is $x = \sum_i a_i M_i N_i$, where $N_i = \frac{N}{n_i}$ and $M_i = N_i^{-1} \bmod n_i$.

The given system of congruences has a solution because $\gcd(4, 3, 5) = 1$. We have $a_1 = 3$, $a_2 = 2$, and $a_3 = 4$. Now we have...

$$\begin{aligned} N &= n_1 n_2 n_3 = 4 \cdot 3 \cdot 5 = 60 \\ N_1 &= \frac{N}{n_1} = \frac{60}{4} = 15 \\ N_2 &= \frac{N}{n_2} = \frac{60}{3} = 20 \\ N_3 &= \frac{N}{n_3} = \frac{60}{5} = 12 \end{aligned}$$

Now we need find the inverses of $15, 20, 12$ with respect to $4, 3, 5$, respectively. First, we reduce these:

$$\begin{aligned} N_1 &= 15 = 3(4) + 3 \equiv 3 \mod 4 \\ N_2 &= 20 = 6(3) + 2 \equiv 2 \mod 3 \\ N_3 &= 12 = 2(5) + 2 \equiv 2 \mod 5 \end{aligned}$$

Now observe that $3(3) = 9 = 2(4) + 1 \equiv 1 \bmod 4$ so that $3^{-1} = 3 \bmod 4$. Furthermore, observe that $2(2) = 4 = 3(1) + 1 \equiv 1 \bmod 3$ so that $2^{-1} = 2 \bmod 3$. Finally, observe that $3(2) = 6 = 1(5) + 1 \equiv 1 \bmod 5$ so that $2^{-1} = 3 \bmod 5$. Therefore, we have...

$$\begin{aligned} M_1 &= 3 \\ M_2 &= 2 \\ M_3 &= 3 \end{aligned}$$

But then a solution the given congruence is...

$$x = \sum_i a_i M_i N_i = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = 3(3)15 + 2(2)20 + 4(3)12 = 135 + 80 + 144 = 359$$

Reducing $x = 359$ modulo $N = 60$, we have $x = 359 = 5(60) + 59 \equiv 59 \bmod 60$. Therefore, the solutions to this system of congruences are $x \equiv 59 \bmod 60$, i.e. the integers of the form $60k + 59$. For example, choosing $k = -2, -1, 0, 1, 2$, we obtain solutions $-85, -25, 35, 95, 155$, respectively. We can also verify these solutions:

$$\begin{aligned} x &= 60k + 59 = 15(4)k + \big(14(4) + 3\big) \equiv 0 + 3 = 3 \equiv 3 \mod 4 \\ x &= 60k + 59 = 20(3)k + \big(19(3) + 2\big) \equiv 0 + 2 = 2 \equiv 2 \mod 3 \\ x &= 60k + 59 = 12(5)k + \big(11(5) + 4\big) \equiv 0 + 4 = 4 \equiv 4 \mod 5 \end{aligned}$$