Name: *Caleb McWhorter — Solutions*
MATH 308
Fall 2023
HW 13: Due 11/10

"The difference between mathematicians and physicists is that after physicists prove a big result they think it is fantastic but after mathematicians prove a big result they think it is trivial."
–Lucien Szpiro

Problem 1. (10pt) Showing all your work, compute the following:

(a) $45 - 69 \mod 27$

(b) $115 + 82 \mod 6$

(c) $11 \cdot 17 \mod 3$

(d) $2^{100} \mod 5$

(e) $-17 \cdot 14 \mod 8$

Solution.

(a) We have $45 - 69 = -24 \equiv 3 \mod 27$ because $-24 = -1(27) + 3$. Alternatively, $45 - 69 \equiv 18 - 15 = 3 \mod 27$.

(b) We have $115+82 = 197 \equiv 5 \mod 6$ because $197 = 32(6)+5$. Alternatively, $115+82 \equiv 1+4 = 5 \mod 6$.

(c) We have $11 \cdot 17 = 187 \equiv 1$ because $187 = 62(3) + 1$. Alternatively, $11 \cdot 17 \equiv 2 \cdot 2 = 4 \equiv 1 \mod 3$.

(d) We have...

$$2^1 = 2 \equiv 2 \mod 5, \qquad 2^2 = (2^1)^2 \equiv 2^2 = 4 \equiv 4 \mod 5, \qquad 2^4 = (2^2)^2 \equiv 4^2 = 16 \equiv 1 \mod 5$$

We then have...

$$2^{100} = (2^4)^{25} \equiv 1^{25} = 1 \mod 5$$

(e) We have $-17 \cdot 14 = -238 \equiv 2 \mod 8$ because $-238 = -30(8) + 2$. Alternatively, we have $-17 \cdot 14 \equiv 7 \cdot 6 = 42 \equiv 2 \mod 8$ or $-17 \cdot 14 \equiv -1 \cdot -2 = 2 \mod 8$.

Problem 2. (10pt) Showing all your work, compute the following:

(a) $\phi(143)$

(b) $\phi(64)$

(c) $\phi(660)$

Solution. Recall that the Euler-ϕ function (or Euler totient function, also denoted φ) is defined as follows: $\phi(n)$ is the number of integers k in the range $1 \leq k \leq n$ such that $\gcd(k, n) = 1$. Recall that if p is prime, then $\phi(p) = p - 1$. Generally, if p is prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$. Finally, if a, b are relatively prime (or coprime), i.e. $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. But if $N = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ is a prime factorization, then...

$$\phi(N) = \phi(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_n^{a_n}) = p_1^{a_1-1}(p_1-1) \cdot p_2^{a_2-1}(p_2-1) \cdot \cdots \cdot p_n^{a_n-1}(p_n-1) = \prod_{i=1}^{n} p_i^{a_i-1}(p_i-1)$$

(a) We have...

$$\phi(143) = \phi(11 \cdot 13) = \phi(11)\phi(13) = (11 - 1)(13 - 1) = 10 \cdot 12 = 120$$

(b) We have...

$$\phi(64) = \phi(2^6) = 2^{6-1}(2 - 1) = 2^5(2 - 1) = 32 \cdot 1 = 32$$

(c) We have...

$$\phi(660) = \phi(2^2 \cdot 3^1 \cdot 5^1 \cdot 11^1) = 2^{2-1}(2-1) \cdot 3^{1-1}(3-1) \cdot 5^{1-1}(5-1) \cdot 11^{1-1}(11-1) = 2(1) \cdot 1(2) \cdot 1(4) \cdot 1(10) = 160$$

Problem 3. (10pt) Showing all your work, complete the following:

(a) The number of digits in 96758^{2023}.

(b) What is the remainder when 19^{115} is divided by 5.

(c) What are the last two digits of 178^{996}?

Solution.

(a) The number of digits in N when expressed in base-b is $\lfloor \log_b N \rfloor + 1$. Recalling the change of base formula $\log_b x = \frac{\ln x}{\ln b}$ and the power formula $\log_b(x^n) = n \log_b x$, we have...

$$\begin{aligned}
\left\lfloor \log_{10}(96758^{2023}) \right\rfloor + 1 &= \lfloor 2023 \log_{10}(96758) \rfloor + 1 \\
&= \left\lfloor 2023 \, \frac{\ln(96758)}{\ln(10)} \right\rfloor + 1 \\
&= \left\lfloor 2023 \cdot \frac{11.47997}{2.302585} \right\rfloor + 1 \\
&= \lfloor 2023 \cdot 4.98569 \rfloor + 1 \\
&= \lfloor 10086.1 \rfloor + 1 \\
&= 10086 + 1 \\
&= 10087
\end{aligned}$$

Therefore, 96758^{2023} has $10{,}087$ digits.

(b) The remainder of N when divided by b is precisely the value of $N \mod b$. Observe that $19 = 20 - 1$, which implies $19 = 20 - 1 \equiv 0 - 1 = -1 \mod 5$. But then we have $19^{115} \equiv (-1)^{115} = -1 \equiv 4 \mod 5$. Therefore, 19^{115} has a remainder of 4 when divided by 5.

(c) The last two digits of an integer N in base-10 is the remainder of N when divided by 100, i.e. the value of $N \mod 100$. Now observe...

$$\begin{aligned}
178^1 &= 178 \equiv 78 \mod 100 & 178^{32} &= (178^{16})^2 \equiv 96^2 = 9216 \equiv 16 \mod 100 \\
178^2 &= (178^1)^2 \equiv 78^2 = 6084 \equiv 84 \mod 100 & 178^{64} &= (178^{32})^2 \equiv 16^2 = 256 \equiv 56 \mod 100 \\
178^4 &= (178^2)^2 \equiv 84^2 = 7056 \equiv 56 \mod 100 & 178^{128} &= (178^{64})^2 \equiv 56^2 \equiv 36 \mod 100 \\
178^8 &= (178^4)^2 \equiv 56^2 = 3136 \equiv 36 \mod 100 & 178^{256} &= (178^{128})^2 \equiv 36^2 \equiv 96 \mod 100 \\
178^{16} &= (178^8)^2 \equiv 36^2 = 1296 \equiv 96 \mod 100 & 178^{512} &= (178^{256})^2 \equiv 92^2 \equiv 16 \mod 100
\end{aligned}$$

Now observe that $996 = 512 + 256 + 128 + 64 + 32 + 4$. But then...

$$\begin{aligned}
178^{996} &= 178^{4+32+64+128+256+512} \\
&= 178^4 \cdot 178^{32} \cdot 178^{64} \cdot 178^{128} \cdot 178^{256} \cdot 178^{512} \\
&\equiv 56 \cdot 16 \cdot 56 \cdot 36 \cdot 96 \cdot 16 \\
&= 2774532096 \\
&\equiv 96
\end{aligned}$$

Therefore, the last two digits of 178^{996} are 96.

Problem 4. (10pt) Consider the congruence $18x + 27 \equiv 5 \mod 31$.

(a) Explain why the given congruence has a solution.

(b) Explain why 18^{-1} exists mod 31.

(c) Solve the congruence and give at least three explicit solutions.

(d) Verify that one of your solutions in (c) is correct.

Solution.

(a) Consider the linear congruence $ax \equiv b \mod n$. Let $\gcd(a, n) = d$. If $d \nmid b$, then there are no solutions. However, if $d \mid b$, there are infinitely many solutions and the solutions are $\frac{xb}{d} + \frac{n}{d}\, z$, where $z \in \mathbb{Z}$ and x is such that for some y, $d = ax + ny$. 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 $1 \leq s \leq n$ such that $s \equiv a^{-1}b$ modulo n. Then general solutions are $x = s + zn$, where $z \in \mathbb{Z}$. We have...

$$\begin{aligned} 18x + 27 &\equiv 5 \mod 31 \\ 18x &\equiv -22 \mod 31 \\ 18x &\equiv 9 \mod 31 \end{aligned}$$

We have $\gcd(18, 31) = 1$ and $1 \mid 9$. Therefore, there is a solution to the given linear congruence.

(b) Let $a, n \in \mathbb{Z}$ with $n > 0$. Suppose that $\gcd(a, n) = d > 1$ and let $dk = a$ and $dk' = n$ for some integers k, k'. Clearly, $k, k' \neq 0$ and $0 \leq k < a$, $0 \leq k' < n$. We know that a^{-1} cannot exist modulo n. If there were an integer, m, such that $ma \equiv 1 \mod n$, then...

$$k' \equiv k' \cdot 1 \equiv k' \cdot ma = k' \cdot m(dk) = (mk) \cdot (dk') = mk \cdot n \equiv mk \cdot 0 \equiv 0$$

Because $k' \equiv 0 \mod n$, we know that $n \mid k'$. But because $0 \leq k' < n$, this is impossible unless $k' = 0$, which is a contradiction. Therefore, there does not exist an integer m such that $ma \equiv 1 \mod n$, i.e. a^{-1} does not exist modulo n.

Now suppose that $\gcd(a, n) = 1$. Given two integers a, b, there exist integers x, y such that $\gcd(a, b) = ax + by$. But then there exists integers x, y such that $ax + ny = 1$. Reducing this modulo n, we have $1 = ax + ny \equiv ax + 0 = ax$. But then x is an integer such that $xa \equiv 1$ modulo n. Therefore, a^{-1} exists.

All the work above shows that a^{-1} exists modulo n if and only if $\gcd(a, n) = 1$. Because $\gcd(18, 31) = 1$, we know that 18^{-1} exists modulo 31.

(c) From (b), we know that 18^{-1} exists modulo 31. Moreover, if x, y are integers such that $ax + ny = 1$, then $x = a^{-1}$ modulo n. We need find integers x, y such that $18x + 31y = 1$. We can find these using the (extended) Euclidean algorithm:

$$\begin{aligned} 31 &= 1(18) + 13 \\ 18 &= 1(13) + 5 \\ 13 &= 2(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \\ 2 &= 2(1) \end{aligned} \qquad \begin{aligned} 1 &= 3 - 1(2) \\ &= 3 - 1\big(5 - 1(3)\big) \\ &= 3 - 1 \cdot 5 + 1 \cdot 3 \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot \big(13 - 2(5)\big) - 1 \cdot 5 \\ &= 2 \cdot 13 - 4 \cdot 5 - 1 \cdot 5 \\ &= 2 \cdot 13 - 5 \cdot 5 \\ &= 2 \cdot 13 - 5\big(18 - 1(13)\big) \\ &= 2 \cdot 13 - 5 \cdot 18 + 5 \cdot 13 \\ &= 7 \cdot 13 - 5 \cdot 18 \\ &= 7\big(31 - 1(18)\big) - 5 \cdot 18 \\ &= 7 \cdot 31 - 7 \cdot 18 - 5 \cdot 18 \\ &= 7 \cdot 31 - 12 \cdot 18 \end{aligned}$$

But then $1 = 7(31) + (-12)18 \equiv 0 + (-12)18 = (-12)18 \mod 31$. Therefore, $18^{-1} = -12 \equiv 19 \mod 31$. We can verify this easily: $19(18) = 342 \equiv 1 \mod 31$. But then...

$$\begin{aligned} 18x + 27 &\equiv 5 \mod 31 \\ 18x &\equiv -22 \mod 31 \\ 18x &\equiv 9 \mod 31 \\ 18^{-1} \cdot 18x &\equiv 18^{-1} \cdot 9 \mod 31 \\ x &\equiv -12 \cdot 9 \mod 31 \\ x &\equiv 19 \cdot 9 \mod 31 \\ x &\equiv 171 \mod 31 \\ x &\equiv 16 \end{aligned}$$

Therefore, the solution modulo 31 is 16. The general solutions are the integers of the form $16 + 31z$, where $z \in \mathbb{Z}$. But then choosing $k = -3, -2, -1, 0, 1, 2, 3$, we know that $-77, -46, -15, 16, 47, 78, 109$ are all solutions to the given equation, respectively.

(d) We select the general solution -77. We have...

$$18x + 27 = 18(-77) + 27 = -1386 + 27 = -1359 \equiv 5 \mod 31,$$

where $-1359 \equiv 5 \mod 31$ because $-1359 = -44(31) + 5$. Alternatively, we could have selected the general solution 109. We have...

$$18x + 27 = 18(109) + 27 = 1962 + 27 = 1989 \equiv 5 \mod 31,$$

where $1989 \equiv 5 \mod 31$ because $1989 = 64(31) + 5$.