Name: *Caleb McWhorter — Solutions*
MATH 308
Fall 2023
HW 12: Due 11/10

"No part of mathematics is ever, in the long run, "useless." Most of number theory has very few "practical" applications. That does not reduce its importance, and if anything it enhances its fascination. No one can predict when what seems to be a most obscure theorem may suddenly be called upon to play some vital and hitherto unsuspected role."

– C. Stanley

Problem 1. (10pt) Showing all your work and fully justifying your answer, complete the following:

(a) From the definition, determine whether 79 is odd or even.

(b) From the definition, determine whether or not -343 a perfect cube.

(c) Find the prime factorization of 840. Find all the divisors of 840.

(d) Can an integer of the form $n^2 + 7n + 6$, where $n \in \mathbb{N}$, be prime? Explain.

Solution.

(a) We know an integer n is odd if there exists an integer k such that $n = 2k + 1$. Observe that taking $k = 39$, we have $2(39) + 1 = 79$. Therefore, 79 is odd. Recall also that an integer n is even if there exists an integer k such that $n = 2k$. Suppose that 79 is even. Then there exists an integer k such that $79 = 2k$. As $78 < 2k < 80$, it must be that $39 < k < 40$. But there is no such integer. Therefore, there is no integer k such that $2k = 79$, so that 79 cannot be even.

(b) An integer n is a perfect cube if there exists an integer k such that $n = k^3$. Observe that taking $k = -7$, we have $(-7)^3 = -343$. Therefore, -343 is a perfect cube.

(c) Observe that $840 = 84 \cdot 10 = (4 \cdot 21) \cdot 10 = \big((2 \cdot 2) \cdot (3 \cdot 7)\big) \cdot (2 \cdot 5) = 2^3 \cdot 3 \cdot 5 \cdot 7$. The prime factorization of 840 is then $2^3 \cdot 3 \cdot 5 \cdot 7$. If $d \mid 840$, then either $d = 1$ or d is a product of prime factors of 840. But then the divisors of 840 are the integers of the form $2^a \cdot 3^b \cdot 5^c \cdot 7^d$, where $a \in \{0, 1, 2, 3\}$ and $b, c, d \in \{0, 1\}$. But then the divisors of 840 are 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 15, 20, 21, 24, 28, 30, 35, 40, 42, 56, 60, 70, 84, 105, 120, 140, 168, 210, 280, 420, 840.

(d) Observe that $n^2 + 7n + 6 = (n + 1)(n + 6)$. For a whole number $n \in \mathbb{N}$, $n + 1$ and $n + 6$ are integers. However, clearly, if $n > 0$, $n + 1$ and $n + 6$ are at least 2. But then $n + 1$ and $n + 6$ are either prime or products of primes by the Fundamental Theorem of Arithmetic. But then $n^2 + 7n + 6 = (n + 1)(n + 6)$ is a product of primes. Therefore, $n^2 + 7n + 6$ cannot be prime.

Problem 2. (10pt) Using the given a, b, express the division $\frac{b}{a}$ using the division algorithm. Be sure to show all your work.

(a) $a = 16$, $b = 2797$

(b) $a = -29$, $b = -7015$

(c) $a = 56$, $b = 55664$

Solution. Recall that the Division Algorithm states that for $a, b \in \mathbb{Z}$ with $a \neq 0$, there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < |a|$ such that $b = qa + r$. If q is known, we can take $r = b - qa$. Recall that we can find q via...

$$q = \begin{cases} \left\lfloor \dfrac{b}{a} \right\rfloor, & a > 0 \\ \\ \left\lceil \dfrac{b}{a} \right\rceil, & a < 0 \end{cases}$$

(a) Because $a > 0$, we have $q = \left\lfloor \dfrac{2797}{16} \right\rfloor = 174$ so that $r = 2797 - 174 \cdot 16 = 2797 - 2784 = 13$. But then we have $2797 = 174(16) + 13$.

(b) Because $a < 0$, we have $q = \left\lceil \dfrac{-7015}{-29} \right\rceil = 242$ so that $r = -7015 - 242(-29) = -7015 + 7018 = 3$. Therefore, $-7015 = 242(-29) + 3$.

(c) Because $a > 0$, we have $q = \left\lfloor \dfrac{55664}{56} \right\rfloor = 994$ so that $r = 55664 - 994 \cdot 56 = 55664 - 55664 = 0$. Therefore, $55664 = 994(56) + 0$.

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

(a) Use the Euclidean Algorithm to find $\gcd(459, 303)$.

(b) Use the extended Euclidean algorithm, express $\gcd(459, 303)$ as a linear combination of 459 and 303.

(c) Is it possible to find integers x, y such that $459x + 303y = 5$? If not, explain why. If so, find them.

(d) Is it possible to find integers x, y such that $459x + 303y = 6$? If not, explain why. If so, find them.

Solution.

(a) Recall that the Euclidean Algorithm computes $\gcd(a, b)$. Each step of the Euclidean Algorithm uses the division algorithm to express $r_{k-2} = q_k r_{k-1} + r_k$, where $0 \leq r_{k-1} < r_k$, and we take $r_{-1} = b$ and $r_{-2} = a$. The algorithm continues until $r_n = 0$ is obtained. We then have $\gcd(a, b) = r_{n-1}$.

$$\begin{aligned}
495 &= 1(303) + 192 \\
303 &= 1(192) + 111 \\
192 &= 1(111) + 81 \\
111 &= 1(81) + 30 \\
81 &= 2(30) + 21 \\
30 &= 1(21) + 9 \\
21 &= 2(9) + 3 \\
9 &= 3(3)
\end{aligned}$$

Therefore, $\gcd(459, 303) = 3$.

(b) Given the outputs of the Euclidean Algorithm, terminating with $r_n = 0$, the extended Euclidean algorithm expresses r_k as a linear combination of r_{k-1} and r_{k-2} beginning with r_{n-1}. When this process terminates, one has expressed $\gcd(a, b)$ as linear combination of a, b.

$$\begin{aligned}
3 &= 21 - 2(9) \\
&= 21 - 2\big(30 - 1(21)\big) \\
&= 21 - 2 \cdot 30 + 2(21) \\
&= 3 \cdot 21 - 2 \cdot 30 \\
&= 3\big(81 - 2(30)\big) - 2 \cdot 30 \\
&= 3 \cdot 81 - 6(30) - 2 \cdot 30 \\
&= 3 \cdot 81 - 8(30) \\
&= 3 \cdot 81 - 8\big(111 - 1(81)\big) \\
&= 3 \cdot 81 - 8 \cdot 111 + 8(81) \\
&= 11 \cdot 81 - 8 \cdot 111 \\
&= 11\big(192 - 1(111)\big) - 8 \cdot 111
\end{aligned}$$

$$
\begin{aligned}
&= 11 \cdot 192 - 11 \cdot 111 - 8 \cdot 111 \\
&= 11 \cdot 192 - 19 \cdot 111 \\
&= 11 \cdot 192 - 19\big(303 - 1(192)\big) \\
&= 11 \cdot 192 - 19 \cdot 303 + 19 \cdot 192 \\
&= 30 \cdot 192 - 19 \cdot 303 \\
&= 30\big(495 - 1(303)\big) - 19 \cdot 303 \\
&= 30 \cdot 495 - 30 \cdot 303 - 19 \cdot 303 \\
&= 30 \cdot 495 - 49 \cdot 303
\end{aligned}
$$

But then we have $3 = 30 \cdot 495 + (-49) \cdot 303$.

(c) Recall that the smallest possible *positive* integer that is expressible as a linear combination of integers a, b is $\gcd(a, b)$; that is, given $a, b \in \mathbb{Z}$, the smallest positive integer of the form $ax + by$, where $x, y \in \mathbb{Z}$, is $\gcd(a, b)$. Furthermore, if $a, b \in \mathbb{Z}$ are nonzero and $n = ax + by$ for some $x, y \in \mathbb{Z}$, then $\gcd(a, b) \mid n$.

By the observations above, if there existed $x, y \in \mathbb{Z}$ such that $459x + 303y = 5$, then $\gcd(459, 303) \mid 5$. We know that $\gcd(459, 303) = 3$. As $3 \nmid 5$, there do not exist integers x, y such that $459x + 303y = 5$.

(d) We know that the extended Euclidean algorithm expresses $\gcd(a, b)$ as a linear combination of a, b. That is, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$. Suppose $\gcd(a, b) \mid n$, i.e. there exists $k \in \mathbb{Z}$ such that $k \gcd(a, b) = n$. But then $n = k \gcd(a, b) = a(kx) + b(ky)$. So if $\gcd(a, b) \mid n$, n is expressible as a linear combination of a, b. We know that $3 = 30 \cdot 495 - 49 \cdot 303$. But then...

$$6 = 2 \cdot 3 = 2\big(30 \cdot 495 - 49 \cdot 303\big) = 60 \cdot 495 - 98 \cdot 303$$

But then $6 = 60 \cdot 495 + (-98) \cdot 303$. Therefore, taking $x = 60$ and $y = -98$, we have $459x + 301y = 6$.

Problem 4. (10pt) Showing all your work, convert the given base-10 number, binary number, or hexadecimal to the given base b:

(a) 7187; $b = 16$

(b) 119; $b = 2$

(c) 11101_2; $b = 10$

(d) 801c; $b = 10$

Solution. There are two obvious approaches to express $N \geq 0$ in base-b. First, one can use a greedy algorithm approach: compute the powers of b that are at most N. Assume these are $b^0, b^1, b^2, \ldots, b^n$. Now for $k \geq 0$, repeatedly apply the division algorithm to express y_k as $y_k = q_k b^{n-k} + r_k$, where $0 \leq r_k < b^{n-k}$, $y_0 = N$, and $y_{k+1} = r_k$. This process terminates at step $n+1$. Expressing q_k in base-b, we have $N = q_0 q_1 \cdots q_n$, so that q_k is the b^{n-k}th's place of N in base-b.

The second method makes this process more 'algorithmic.'We iteratively apply the division algorithm: to express N in base b, for $k \geq 1$, we express b_k as $b_k = q_k b + r_k$ until $b_k = 0$, where q_k, r_k are found by applying the division algorithm to b_k and 16, $b_1 = N$, and $b_{k+1} = q_k$. If this process terminates at step n, then in base-b, $N = r_n r_{n-1} \cdots r_1$, so that r_i is the b^{i-1}th's place of N in base-b.

(a) Using the first method, observe that $16^0 = 1$, $16^1 = 16$, $16^2 = 256$, and $16^3 = 4096$. Now $7187/16^3 = 7187/4096 \approx 1.75$ and $7187 - 1(4096) = 3091$. Now $3091/16^2 = 3091/256 \approx 12.07$ and $3091 - 12(256) = 19$. [Note that in base-16, 12 = c.] Now $19/16^1 = 19/16 \approx 1.19$ and $19 - 1(16) = 3$. Finally, $3/16^0 = 3/1 = 3$ and $3 - 3(1) = 0$. Therefore, $7187_{10} = 1c13_{16}$. Using the second method, we have...

16	7187	
	449	3
	28	1
	1	$12 = \text{c}_{16}$
	0	1

$$7187_{10} = 1c13_{16}$$

(b) Using the first method, observe that $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, and $2^6 = 64$. Now $119/2^6 = 119/64 \approx 1.86$ and $119 - 1(64) = 55$. Then $55/2^5 = 55/32 = 1.72$ and $55 - 1(32) = 23$. Then $23/2^4 = 23/16 = 1.44$ and $23 - 1(16) = 7$. Then $7/2^3 = 7/8 = 0.875$ and $7 - 0(8) = 7$. Then $7/2^2 = 7/4 = 1.75$ and $7 - 1(4) = 3$. Then $3/2^1 = 3/2 = 1.5$ and $3 - 1(2) = 1$. Finally, $1/2^0 = 1/2 = 0.5$ and $1 - 0(2) = 1$. Therefore, $119_{10} = 1110111_2$. Using the second method, we have...

$$\begin{array}{r|r|l} 2 & 119 & \\ \cline{2-3} & 59 & 1 \\ & 29 & 1 \\ & 14 & 1 \\ & 7 & 0 \\ & 3 & 1 \\ & 1 & 1 \\ & 0 & 1 \end{array}$$

$$119_{10} = 1110111_2$$

(c) Recall to express $N_b = a_n a_{n-1} \cdots a_1 a_0$ in base-10, we compute $\sum_{i=0}^{n} a_i \cdot b^i$, where a_i and b_i are expressed in base-10. We then have. . .

$$\begin{aligned} 11101_2 &= 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 \\ &= 1 \cdot 1 + 0 \cdot 2 + 1 \cdot 4 + 1 \cdot 8 + 1 \cdot 16 \\ &= 1 + 0 + 4 + 8 + 16 \\ &= 29 \end{aligned}$$

(d) Recall to express $N_b = a_n a_{n-1} \cdots a_1 a_0$ in base-10, we compute $\sum_{i=0}^{n} a_i \cdot b^i$, where a_i and b_i are expressed in base-10. Recall also that when expressed in base-10, the base-16 (hexadecimal) numbers a–f are a $= 10$, b $= 11$, c $= 12$, d $= 13$, e $= 14$, and f $= 15$. We then have. . .

$$\begin{aligned} 801\text{c}_{16} &= c_{16} \cdot 16^0 + 1 \cdot 16^1 + 0 \cdot 16^2 + 8 \cdot 16^3 \\ &= 12 \cdot 1 + 1 \cdot 16 + 0 \cdot 256 + 8 \cdot 4096 \\ &= 12 + 16 + 0 + 32768 \\ &= 32796 \end{aligned}$$