Name: *Caleb McWhorter — Solutions*
MATH 308
Fall 2022
HW 13: Due 11/10

"...there is no apparent reason why one number is prime and another not. To the contrary, upon looking at these numbers one has the feeling of being in the presence of one of the inexplicable secrets of creation."
–Don Zagier

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

(a) Using the definition of even, show that -484 is even.

(b) Using the definition of odd, show that 151 is odd.

(c) Find the prime factorization of 360.

(d) Find all the prime divisors of 45!.

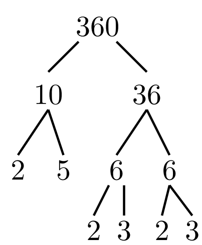
(e) Can an integer of the form $n^4 - 9$, where $n \in \mathbb{Z}$, be prime?

Solution.

(a) We know that an integer n is even if there exists $k \in \mathbb{Z}$ such that $n = 2k$. Because $-484 = 2(-242)$, we know that k is even.

(b) An odd integer is an integer that is not even, i.e. n is odd if there does not exist an integer k such that $n = 2k$. If there were such a k for 151, we would have $151 = 2k$. But this implies that $k = \frac{151}{2} \notin \mathbb{Z}$, a contradiction. Therefore, 151 cannot be even so that 151 is odd. Alternatively, we know that an integer n is odd if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. Observe that $151 = 2(75) + 1$. Therefore, 151 is odd.

(c) We have...



Therefore, $360 = 2^3 \cdot 3^2 \cdot 5$.

(d) We have $45! = 45 \cdot 44 \cdot 43 \cdot \cdots \cdot 2 \cdot 1$. Therefore, by Euclid's Theorem, if $p \mid 45!$, then $p \mid k$, where $1 \leq k \leq 45$. But then p is a divisor of one of the integers from 1 to 45. Conversely, because each prime divisor of k, where $1 \leq k \leq 45$, occurs as an integer in the product $45!$, we know that each such prime divisor occurs. Therefore, $p \mid 45!$ if and only if it is a prime number less than 45. The prime numbers less than 45 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, and 43.

(e) Because $n^4 - 9 = (n^2 - 3)(n^2 + 3)$, if $n^4 - 9$ is prime, then one of $n^2 - 3$ or $n^2 + 3$ is ± 1. Clearly, $n^2 + 3 \geq \pm 1$. Therefore, it must be that $n^2 - 3 = \pm 1$, i.e. $n^2 = 4$ or $n^2 = 2$. The latter case implies $n = \pm\sqrt{2}$, which is not an integer. In the former, we have $n = \pm 2$. We can check that if $n = \pm 2$, then $n^4 - 9 = 7$, which is prime. Conversely, if $n \neq \pm 2$, then $n^2 - 3 \neq \pm 1$ and $n^2 + 3 \geq 1$ so that $(n^2 - 3)(n^2 + 3) = n^4 - 9$ is not prime. Therefore, $n^4 - 9$ is prime when $n = \pm 2$, and is composite otherwise.

Problem 2. (10pt) Showing all your work and fully justifying your reasoning, complete the following:

(a) List at least ten multiples of 17.

(b) List the divisors of 120.

(c) What are the prime divisors of 120?

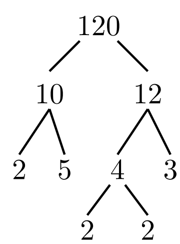
Solution.

(a) The multiples of 17 are the integers of the form $17k$, where $k \in \mathbb{Z}$. Choosing $k = -5, -4, \ldots, 5$, we obtain...

$$-85,\ -68,\ -51,\ -34,\ -17,\ 0,\ 17,\ 34,\ 51,\ 68,\ 55$$

(b) The divisors of 120 are the integers a such that $a \mid 120$. But then the divisors of 120 are 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, and 120. Alternatively, finding the prime factorization of 120, we obtain $120 = 2^3 \cdot 3^1 \cdot 5^1$. Then the divisors of 120 are the integers of the form $2^a \cdot 3^b \cdot 5^c$, where $0 \leq a \leq 3$, $0 \leq b \leq 1$, and $0 \leq c \leq 1$.

(c) The prime divisors of 120 are the integers a such that $a \mid 120$ and a is prime. We find the prime factorization of 120:



Therefore, $120 = 2^3 \cdot 3 \cdot 5$. Then the prime divisors of 120 are 2, 3, and 5.

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

(a) By enumerating the divisors of 40 and 100, compute $\gcd(40, 100)$.

(b) By enumerating sufficient multiples of 25 and 60, compute $\operatorname{lcm}(25, 60)$.

(c) Compute $\gcd(2^{100} \cdot 3^{200} \cdot 5^{600} \cdot 11^{100},\ 2^{300} \cdot 3^{100} \cdot 5^{600} \cdot 7^{800})$.

(d) Compute $\operatorname{lcm}(2^{100} \cdot 3^{200} \cdot 5^{600} \cdot 11^{100},\ 2^{300} \cdot 3^{100} \cdot 5^{600} \cdot 7^{800})$.

Solution.

(a) Enumerating the divisors of 40 and 100, we have...

$$40\colon 1,\ 2,\ 4,\ 5,\ 8,\ 10,\ \mathbf{20},\ 40$$
$$100\colon 1,\ 2,\ 4,\ 5,\ 10,\ \mathbf{20},\ 25,\ 50,\ 100$$

Therefore, $\gcd(40, 100) = 20$.

(b) Enumerating multiples of 25 and 60, we have...

$$25\colon 0,\ 25,\ 50,\ 75,\ 100,\ 125,\ 150,\ 175,\ 200,\ 225,\ 250,\ 275,\ \mathbf{300},\ 325,\ 350,\ 375,\ \ldots$$
$$60\colon 0,\ 60,\ 120,\ 180,\ 240,\ \mathbf{300},\ 360,\ 420,\ 480,\ 540,\ 600,\ 660,\ 720,\ 780,\ 840,\ 900,\ \ldots$$

Therefore, $\operatorname{lcm}(25, 60) = 300$.

(c) Using the fact that if $a = \prod_{i=1}^{n} p_i^{a_i}$ and $b = \prod_{i=1}^{n} p_i^{b_i}$, where the p_i are prime and $a_i, b_i \geq 0$, then $\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$, we have...

$$\gcd(2^{100} \cdot 3^{200} \cdot 5^{600} \cdot 11^{100},\ 2^{300} \cdot 3^{100} \cdot 5^{600} \cdot 7^{800}) = 2^{100} \cdot 3^{100} \cdot 5^{600} \cdot 7^{0} \cdot 11^{0} = 2^{100} \cdot 3^{100} \cdot 5^{600}$$

(d) Using the fact that if $a = \prod_{i=1}^{n} p_i^{a_i}$ and $b = \prod_{i=1}^{n} p_i^{b_i}$, where the p_i are prime and $a_i, b_i \geq 0$, then $\operatorname{lcm}(a, b) = \prod_{i=1}^{n} p_i^{\max(a_i, b_i)}$, we have...

$$\gcd(2^{100} \cdot 3^{200} \cdot 5^{600} \cdot 11^{100},\ 2^{300} \cdot 3^{100} \cdot 5^{600} \cdot 7^{800}) = 2^{300} \cdot 3^{200} \cdot 5^{600} \cdot 7^{800} \cdot 11^{100}$$

Problem 4. (10pt) Showing all your work and justifying your reasoning, complete the following:

(a) Prove or disprove: if p is prime, then $p^2 + 1$ is also prime.

(b) Using the fact that $ab = \mathrm{lcm}(a, b) \cdot \gcd(a, b)$ and $\gcd(196, 1320) = 4$, compute $\mathrm{lcm}(196, 1320)$.

(c) If $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = p$, where p is prime, what are the possible values for $\gcd(a^2, b)$, $\gcd(a, b^2)$, $\gcd(a^2, b^2)$, and $\gcd(a^2, b^3)$?

Solution.

(a) The statement is false. For instance, $p = 3$ is prime but $3^2+1 = 10$ is not prime, i.e. composite.

(b) We have...

$$\mathrm{lcm}(196, 1320) = \frac{196 \cdot 1320}{\gcd(196, 1320)} = \frac{258720}{4} = 64680$$

(c) If $\gcd(a, b) = p$ is prime, then we know that $p \mid a$ and $p \mid b$. But then we can write $a = Ap^r$ and $b = Bp^s$, where $A, B, r, s \in \mathbb{Z}$, $\gcd(A, p) = 1$, $\gcd(B, p) = 1$, and $r, s \geq 1$. Clearly, we cannot have $r, s \geq 2$ simultaneously; otherwise, we would have $\gcd(a, b) = \gcd(Ap^r, Bp^s) \geq p^2$, a contradiction.

Then we have $\gcd(a^2, b) = \gcd(A^2p^{2r}, Bp^s) = p^{\min(2r,s)}$. Because $r, s \geq 1$ and one of r, s is 1, we know that $\min(2r, s) \in \{1, 2\}$. Therefore, $\gcd(a^2, b) \in \{p, p^2\}$.

Similarly, we have $\gcd(a, b^2) = \gcd(Ap^r, B^2p^{2s}) = p^{\min(r,2s)}$. Because $r, s \geq 1$ and one of r, s is 1, we know that $\min(r, 2s) \in \{1, 2\}$. Therefore, $\gcd(a, b^2) \in \{p, p^2\}$.

We also have $\gcd(a^2, b^2) = \gcd(A^2p^{2r}, B^2p^{2s}) = p^{\min(2r,2s)} = p^{2\min(r,s)}$. Because $r, s \geq 1$ and one of r, s is 1, we know $2\min(r, s) = 2 \cdot 1 = 2$. Therefore, $\gcd(a^2, b^2) = p^2$.

Finally, we have $\gcd(a^2, b^3) = \gcd(A^2p^{2r}, B^3p^{3s}) = p^{\min(2r,3s)}$. Because $r, s \geq 1$ and one of r, s is 1, we know $\min(2r, 3s) \in \{2, 3\}$. Therefore, $\gcd(a^2, b^3) \in \{p^2, p^3\}$.