ORMC AMC Group: Week 3 Solutions
Number Theory

October 9, 2022

1 Euclidean Algorithm Solutions

1. Find a pair of integers (a, b) such that $2022a + 1003b = 1$.The most methodical way of doing this uses the Euclidean Algorithm. So let's start by writing out the steps:

$$2022 = 2 \cdot 1003 + 16$$

$$1003 = 62 \cdot 16 + 11$$

$$16 = 1 \cdot 11 + 5$$

$$11 = 2 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0$$

Now, we rewrite each of these equations (except for the last one) in terms of the remainder. The idea behind doing this is to start with 1 and work our way back up the equations, substituting until we have an expression in terms of 2022 and 1003.

$$16 = 2022 - 2 \cdot 1003$$

$$11 = 1003 - 62 \cdot 16$$

$$5 = 16 - 1 \cdot 11$$

$$1 = 11 - 2 \cdot 5$$

First, we substitute for 5 in the last equation:

$$1 = 11 - 2 \cdot (16 - 1 \cdot 11) = 11 - 2 \cdot 16 + 2 \cdot 11 = 3 \cdot 11 - 2 \cdot 16$$

Then, substitute for 11:

$$1 = 3 \cdot (1003 - 62 \cdot 16) - 2 \cdot 16 = 3 \cdot 1003 - 186 \cdot 16 - 2 \cdot 16 = 3 \cdot 1003 - 188 \cdot 16$$

Finally, substitute for 16:

$$1 = 3 \cdot 1003 - 188 \cdot (2022 - 2 \cdot 1003) = 3 \cdot 1003 - 188 \cdot 2022 + 376 \cdot 1003 = 379 \cdot 1003 - 188 \cdot 2022$$

So, we have $a = -188$ and $b = 379$.

Note that all solutions will be of the form $a = -188 + 1003k, b = 379 - 2020k$.

2. (**IMO 1959 #1, modified**) For what integer values of n is $\dfrac{21n + 4}{14n + 3}$ irreducible?

As discussed in class, we simply apply the Euclidean algorithm to these two expressions:

$$21n + 4 = 1(14n + 3) + (7n + 1)$$

$$14n + 3 = 2(7n + 1) + 1$$

$$7n + 1 = (7n + 1)(1) + 0$$

This means that the gcd of $21n + 4$ and $14n + 3$ is 1, no matter what n is.

So the fraction irreducible for all integers n.

3. (**2020 AMC 10A #24**) Let n be the least positive integer greater than 1000 for which

$$\gcd(63, n+120) = 21 \quad \text{and} \quad \gcd(n+63, 120) = 60.$$

What is the sum of the digits of n?

We use the Euclidean Algorithm to simplify this slightly, but only because it preserves gcd's. That is, we can say $\gcd(63, n+120) = \gcd(63, n+120-63) = \gcd(63, n+57)$ and $\gcd(n+63, 120) = \gcd(n+63-120, 120) = \gcd(n-57, 120)$.

This then implies that $n+57 = 21a$, where a is relatively prime to 3, and $n-57 = 60b$, where b is relatively prime to 2. In particular b must be odd, so we can write $b = 2c+1$.

Plugging in, we have $n+57 = 21a$ and $n-57 = 120c+60$. We can eliminate n by subtracting the equations, which gives us

$$2 \cdot 57 = 21a - 120b - 60 \implies 2 \cdot 19 = 7a - 40c - 20$$

We can also change to working $\mod 40$ in order to "eliminate" c, which gives us:

$$38 \equiv 7a - 20 \pmod{40} \implies 7a \equiv 18 \pmod{40}$$

Note that $7^2 = 49 \equiv 9$, and 9 is its own inverse $\mod 40$. So $7^{-1} \equiv 7 \cdot 9 \equiv 63 \equiv 23 \pmod{40}$. This gives us $a \equiv 18 \cdot 23 \equiv 14 \pmod{40}$, so we can write $a = 40d + 14$.

Since $a \not\equiv 0 \pmod 3$, we must have $40d + 14 \equiv d + 2 \not\equiv 0 \implies d \not\equiv 1$, which means the smallest possible value of d is 2. This gives us $a = 94 \implies n = 1917$. So, the sum of the digits is $1+9+1+7 = 18$.

2 Prime Factorization Solutions

1. Show that if $m, n \in \mathbb{Z}$ and $ma + nb > 0$, then $ma + nb \geq \gcd(a, b)$.

   As mentioned in class, if $\gcd(a, b) = d$, then we can write $a = xd, b = yd$ for some $x, y \in \mathbb{Z}$. So, if $ma + nb > 0$, then $mxd + nyd > 0 \implies d(mx + ny) > 0 \implies mx + ny > 0$. But since all of m, x, n, y are integers, this means $mx + ny \geq 1 \implies d(mx + ny) \geq d$.

2. How many even factors does 15! have? How many square factors?

   Let's start with the prime factorization:

   $$15! = (3 \cdot 5)(2 \cdot 7)(13)(2^2 \cdot 3)(11)(2 \cdot 5)(3^2)(2^3)(7)(2 \cdot 3)(5)(2^2)(3)(2)$$
   $$= 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$$

   If n is divisible by p^r, then any divisor of n may be divisible by p^s, where $0 \leq s \leq r$. So for each p^r in the factorization above, the prime factorization of a divisor of 15! may have p raised to any power from 0 to r. This gives us $r + 1$ choices.

   So, in total, we have $(11 + 1)(6 + 1)(3 + 1)(2 + 1)(1 + 1)(1 + 1) = 4032$ divisors. What makes a divisor even? It must be divisible by 2. This means the power on the 2 in its prime factorization must be greater than 0. So our options for all the rest of the numbers remain the same, but we have one less option for the exponent on the 2, giving us:

   $$11 \cdot 7 \cdot 4 \cdot 3 \cdot 2 \cdot 2 = 3696 \text{ even divisors}$$

   What makes a divisor a perfect square? As discussed in class, it is a perfect square when all the exponents in its prime factorization are even. So, the exponent on the 2 may be any of $\{0, 2, 4, 6, 8, 10\}$, and the exponent on the 3 may be any of $\{0, 2, 4, 6\}$, and so on. Applying this to all the exponents gives us:

   $$6 \cdot 4 \cdot 2 \cdot 2 \cdot 1 \cdot 1 = 96 \text{ square divisors}$$

3. (**2018 AMC 10B #23**) How many ordered pairs (a, b) of positive integers satisfy the equation

   $$a \cdot b + 63 = 20 \cdot \text{lcm}(a, b) + 12 \cdot \gcd(a, b)?$$

   Recall the definitions of lcm and gcd from the worksheet, and note that $\text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$. So, letting $L = \text{lcm}(a, b), G = \gcd(a, b)$ we may simply rewrite the above equation as $LG + 63 = 20L + 12G$.

   Using the factoring trick from week 1, we have

   $$LG - 20L - 12G + 63 = 0 \implies LG - 20L - 12G + 240 = 240 - 63 = 177$$
   $$\implies (L - 12)(G - 20) = 177$$

   The prime factorization of 177 is $3 \cdot 59$, and $G \leq L$ by the definitions of gcd and lcm, so the only possible values for (G, L) are $(1 + 20, 177 + 12)$ and $(3 + 20, 59 + 12)$.

   Now, we briefly revisit the definitions of lcm and gcd to complete the problem. Recall that

   $$a = p_1^{m_1} \cdots p_k^{m_k}, \quad b = p_1^{n_1} \cdots p_k^{n_k}$$
   $$\implies \gcd(a, b) = p_1^{\min(m_1, n_1)} \cdots p_k^{\min(m_k, n_k)}, \quad \text{lcm}(a, b) = p_1^{\max(m_1, n_1)} \cdots p_k^{\max(m_k, n_k)}.$$

   So, if we start with the lcm and gcd, then for each prime where the exponent is different between lcm and gcd, we may choose to give the max value to a and min to b, or vice versa.

   For example, if $\text{lcm} = 2^3 \cdot 3 \cdot 5^2$ and $\gcd = 2 \cdot 3$, then we may reconstruct a, b by going through the primes one-by-one. Starting with 2, one of them has an exponent of 3 and the other has an exponent of 1. This gives us 2 choices. For 3, both must have an exponent of 1, so we only have

1 choice here. Finally, for 5, one has an exponent of 0 and the other has an exponent of 2, giving us another 2 choices. So, there are $2 \cdot 2 = 4$ possible ordered pairs a, b:

$$\{(2{\cdot}3, 2^3{\cdot}3{\cdot}5^2), (2{\cdot}3{\cdot}5^2, 2^3{\cdot}3), (2^3{\cdot}3, 2{\cdot}3{\cdot}5^2), (2^3{\cdot}3{\cdot}5^2, 2{\cdot}3)\} = \{(6, 600), (150, 24), (24, 150), (600, 6)\}.$$

Applying this to our situation, we first examine $G = 21, L = 189$. We have $21 = 3 \cdot 7$ and $L = 3^3 \cdot 7$. These prime factorizations only differ on the 3, so there are only 2 possible ordered pairs here.

Moving on to $G = 23, L = 71$. It is easy to check that both of these are prime, but from the definition of lcm and gcd, it is clear that the gcd must divide the lcm. So this is not possible, and we can ignore this case.

Thus, we are left with 2 total ordered pairs a, b.

4. If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, then what is $\gcd(ab, c)$? What about when $\gcd(a, c) = d > 1$?

   Note that $\gcd(m, n) = 1$ if and only if the prime factorizations of m, n share no primes. So if $\gcd(a, c) = \gcd(b, c) = 1$, then b shares no primes with c, and a shares no primes with c, so ab must not share any primes with c either, giving us $\gcd(ab, c) = 1$.

   Similarly, if $gcd(a, c) = d > 1$ but $\gcd(b, c) = 1$, then multiplying b by a cannot add any more prime factors that might be shared with c. So, $\gcd(ab, c) = d$.

   It is important to note that for a result like this to hold, one of $\gcd(a, c)$ or $\gcd(b, c)$ must be 1. Otherwise, we have to deal with cases like $a = 6, b - 9, c = 18$ where $\gcd(a, c) = 6$, $\gcd(b, c) = 9$, and $\gcd(ab, c) = 18$.

5. (**2018 AMC 10A #22**) Let a, b, c, and d be positive integers such that $gcd(a, b) = 24, gcd(b, c) = 36, gcd(c, d) = 54$, and $70 < gcd(d, a) < 100$. Which of the following must be a divisor of a?

   (A) 5 (B) 7 (C) 11 (D) 13 (E) 17

   Start with the prime factorizations of the given numbers:

   $$24 = 2^3 \cdot 3 \quad 36 = 2^2 \cdot 3^2 \quad 54 = 2 \cdot 3^3.$$

   We have 24 divides a, $\text{lcm}(24, 36)$ divides b, $\text{lcm}(36, 54)$ divides c, and 54 divides d. So, we may rewrite each of them in the following way:

   $$a = 24k = 2^3 \cdot 3 \cdot k$$

   $$b = 72l = 2^3 \cdot 3^2 \cdot l$$

   $$c = 108m = 2^2 \cdot 3^3 \cdot m$$

   $$d = 54n = 2 \cdot 3^3 \cdot n$$

   Note that $\gcd(a, d) = 2{\cdot}3{\cdot}\gcd(k, n)$. Note also that 3 cannot divide k, or else $\gcd(a, b) \geq 2^3 \cdot 3^2 = 72$. Similarly, 2 cannot divide n, or else $\gcd(c, d) \geq 2^2 3^3 = 108$. This means that neither 2 nor 3 may divide $\gcd(k, n)$.

   But we know that $\gcd(a, d)$ is a multiple of 6 between 70 and 100, which means that $\gcd(k, n) \in \{12, 13, 14, 15, 16\}$. The only one of these values not divisible by 2 or 3 is 13, so our answer is (D) 13.

3 Modular Arithmetic Solutions

1. Let $\overline{a_n \cdots a_1 a_0}$ represent the number with digits $a_n, a_{n-1}, \ldots, a_1, a_0$.
   Find k such that if $\overline{a_n \cdots a_1 a_0} \equiv 0 \pmod{17}$, then $\overline{a_n \cdots a_1} - ka_0 \equiv 0 \pmod{17}$.

   The first thing to do, like last week's similar exercise, is to rewrite this. If we let $\overline{a_n \cdots a_1 a_0} = X$, then $\overline{a_n \cdots a_1} = (X - a_0)/10$. Now, we have to fix the /10, since we can't "divide" in modular arithmetic. So, we find $10^{-1} \pmod{17}$, which we can easily check is 12, as $12 \cdot 10 = 120 = 119 + 1 = 7 \cdot 17 + 1$. (You can find this inverse by remembering that $7 \cdot 7$ ends with a 9, which means the next multiple of 10 would be congruent to $1 \pmod{17}$.) Then, we just have to rewrite and solve:

$$X \equiv 0 \pmod{17}, \quad 12(X - a_0) - ka_0 \equiv 0 \implies 12X - 12a_0 - a_0 \equiv 0$$

$$\implies 12a_0 + ka_0 \equiv 0 \implies 12 + k \equiv 0 \implies k \equiv -12 \equiv 5 \pmod{17} \implies k = 17n + 5, \forall n \in \mathbb{Z}$$

2. (**AMC 12B 2010 #16**) Positive integers a, b, and c are randomly selected with replacement from the set $\{1, 2, 3, \ldots, 2010\}$. What is the probability that $abc + ab + a$ is divisible by 3?

   Note first that 2010 is divisible by 3, so it would be equivalent to just consider $abc + ab + a$ mod 3, where a, b, c are random values mod 3 (i.e., completely ignoring the 2010).

   Note that if $a \equiv 0 \mod 3$, which happens with probability $1/3$, then the requirement is satisfied. If not, then a have: has an inverse mod 3, so we have:

$$a(bc + c) + a \equiv 0 \mod 3$$

$$a(bc + c) \equiv -a \mod 3$$

$$c(b + 1) \equiv -1 \equiv 2 \mod 3$$

   Which, we can check easily (since there are only 3 possible values) happens precisely when $b \equiv c \equiv 2$ or $b \equiv 0, c \equiv 2$. This gives us 2 choices for the values of b and $c \pmod 3$, and we additionally have 2 choices for the value of $a \pmod 3$. There are a total of $3 \cdot 3 \cdot 3 = 27$ choices for the values of a, b, c, so this case happens with probability $(2 \cdot 2)/27 = 4/27$.

   Thus, the total probability is $1/3 + 4/27 = 13/27$.

3. (**AMC 12A 2010 #23**) The number obtained from the last two nonzero digits of 90! is equal to n. What is n?

   Note that this is equivalent to dividing out all factors of 10 from 90!, and then finding the remainder when the resulting number is divided by 100. Since factors of 5 occur much less often than factors of 2, dividing out all factors of 10 would be equivalent to dividing out all factors of 5, and then dividing out 2 the same number of times. Since 90 is so large, it is clear that there are *many* more factors of 2 than 5. In particular, even after we divide out all factors of 10, the resulting number should be divisible by 4. This means, by the chinese remainder theorem, we really only have to worry about mod 25, after we divide out all the factors of 10.

   Now, let's think about what the factorial would look like after we remove all the multiples of 5:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 1 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 2 \cdots 88 \cdot 89 \cdot 18$$

   Notice that the numbers are coming in groups of 4, and that the $5th$ number is changed (since we removed all factors of 5). We can use this to our advantage, and try to find some repeating pattern.

   The first four unchanged numbers form 4!, which is $24 \equiv -1 \pmod{25}$. What about the next chunk? $6 \cdot 7 \cdot 8 \cdot 9 \equiv 54 \cdot 56 \equiv 4 \cdot 6 \equiv 24 \equiv -1 \pmod{25}$. It's the same! Notice that we multiplied the first and last term $(6 \cdot 9)$, and the middle two terms $(7 \cdot 8)$, before combining them. This is a good technique in general because it helps keep the numbers you are working with small, and around the same size. In this case, it also led us to some potential extra insight. It seems that the first and last number multiply to $4 \pmod{25}$ and the middle two numbers multiply to $6 \pmod{25}$. We can check that this is true in general:

In general, the numbers in the chunks are $5n+1, 5n+2, 5n+3, 5n+4$. The product of the first and last numbers is $25n^2 + 20n + 5n + 4 = 25n^2 + 25n + 4 \equiv 4$. Similarly, the product of the middle two numbers is $25n^2 + 15n + 10n + 6 = 25n^2 + 25n + 6 \equiv 6$. So this will work for all chunks, and we can simply replace each chunk with $-1 \pmod{25}$.

This means our factorial simplifies to:

$$(-1)^{18}(1 \cdot 2 \cdot 3 \cdot 4) \cdot 1 \cdot (6 \cdot 7 \cdot 8 \cdot 9) \cdot 2 \cdot (11 \cdot 12 \cdot 13 \cdot 14) \cdot 3 \cdot (16 \cdot 17 \cdot 18) \pmod{25}$$

Remember that up to this point, we have removed all the factors of 5, but we have not removed the corresponding factors of 2. Now would be a good time to do so. We have 18 multiples of 5 from 1 to 90, and 3 multiples of 25, giving us a total of $18+3 = 21$ factors of 5 in 90!. So, we have 21 factors of 2 to remove. However, recall by Euler's Totient theorem that $2^{20} \equiv 1 \pmod{25}$, so we really only have one factor of 2 to remove, which we can remove from the 18. Doing this removal and then simplifying the expression above again, we get:

$$(-1) \cdot 1 \cdot (-1) \cdot 2 \cdot (-1) \cdot 3 \cdot (16 \cdot 17 \cdot 9) \equiv (-1)^3 \cdot 6 \cdot 9 \cdot 16 \cdot 17 \equiv -1 \cdot 54 \cdot 16 \cdot 17$$

$$\equiv (4 \cdot 16) \cdot (-1 \cdot 17) \equiv 64 \cdot 8 \equiv 512 \equiv 12 \pmod{25}$$

So, this means that once we divide all the factors of 10 out of 90!, we end up with a number x satisfying $x \equiv 0 \pmod{4}$ and $x \equiv 12 \pmod{25}$. Since $12 \equiv 0 \pmod{4}$, the chinese remainder theorem tells us that $x \equiv 12 \pmod{100}$, so our final answer is 12.

4. Let $Rem_m(S)$ denote the set of remainders $0 \leq r < m$ produced when each element of S is divided by m. For example,

$$Rem_3(\{5, 9, 14, 28, 14, 12\}) = \{2, 0, 2, 1, 2, 0\} = \{0, 1, 2\}.$$

What is $Rem_n(\{0, a, 2a, 3a \ldots, (n-1)a\})$, when $\gcd(a, n) = 1$?

First, try some example numbers. For example, try $a = 2, n = 5$. Try some trivial examples like $a = 1, n = 8$, as well. You may notice that $Rem_n(\{0, a, 2a, \ldots, (n-1)a\}) = \{0, 1, 2, \ldots, n-1\}$ for all the examples you try. I claim that this is always true.

We will show that this is the case in a proof by contradiction (your work does not have to be this formal, but I am providing a full proof in order to remove any doubt in your mind that my claim is true):

Proof. For convenience, let S denote $\{0, a, 2a, \ldots, (n-1)a\}$. Assume, for the sake of contradiction, that there is some pair a, n that we can pick, such that $\gcd(a, n) = 1$, and $Rem_n(S) \neq \{0, 1, 2, \ldots, n-1\}$. This means that there is some remainder $0 \leq r < n$ that never appears in $Rem_n(S)$. In particular, there are fewer than n elements in $Rem_n(S)$.

However, there were n elements in S, and each of them has some remainder when divided by n. This means that at least 2 elements of S had the same remainder when divided by n. Without less of generality, let these elements be ax and ay.

Since they have the same remainder when divided by n, we may write them as $ax = q_x n + r$ and $ay = q_y n + r$. Note that their difference is $(q_x - q - y)n$, so it is divisible by n.

However, their difference can also be written as $a(x-y)$. Recall that $\gcd(a, n) = 1$, and that x and y are both less than n. In particular, $\gcd(x-y, n) \leq x - y < n$, since the gcd of two numbers must be less than both of those numbers. But then, by exercise 4 from the prime factorization exercises above, $\gcd(a(x-y), n) = \gcd(x-y, n) < n$, which means that n cannot possibly divide the difference between these two numbers.

This contradiction means that our original assumption must have been false. That is, whenever $\gcd(a, n) = 1$, we must have $Rem_n(S) = \{0, 1, 2, \ldots, n-1\}$. □

4 Chinese Remainder Theorem Solutions

1. Mr. Yu wants to divide the class into groups. When he tries to divide into groups of 3, 1 student is left over. When he tries to divide into groups of 4, 1 student is left over. And when he tries to divide into groups of 5, 1 student is left over. What is the least number of students he could have, assuming he has more than 1 student?

   First, we set up a system of congruences based on this problem. Let N be the number of students in the class. Then:

   $$N \equiv 1 \pmod 3$$
   $$N \equiv 1 \pmod 4$$
   $$N \equiv 1 \pmod 5$$

   Now, we could go ahead and solve this the way we did some examples in class. However, it is easier to just notice that $N = 1$ solves all of these congruences. Then, since the chinese remainder theorem tells us that any solution is unique $\pmod{60}$ $(3 \cdot 4 \cdot 5 = 60)$, this means we are done, and the solution is $N \equiv 1 \pmod{60}$. In particular, N=$60k + 1$, for some integer k. If there must be more than 1 student, then the smallest possible number of students would be 60+1=61.

2. (**AMC 12B 2017 #19**) Let $N = 123456789101112 \ldots 4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

   45 is a bit unwieldy to work with as a modulus, but we can split it up into 9 and 5 and work with those via the chinese remainder theorem. Notice that $N \equiv 4 \pmod 5$, and that the sum of the digits, $\pmod 9$ will be congruent to $1 + 2 + \ldots + 44 = \frac{44 \cdot 45}{2} = 22 \cdot 5 \cdot 9 \equiv 0 \pmod 9$. So, $N \equiv 4 \pmod 5$ and $N \equiv 0 \pmod 9$, and the smallest number satisfying both of these conditions is 9.

   That means the remainder when we divide N by 45 is 9, by the Chinese Remainder Theorem.

3. Find the least positive integer n for which $2^n + 5^n - n$ is a multiple of 1000.

   This solution is incredibly tricky, and I left this as a harder challenge problem. However, the main idea here is to (implicitly) use Chinese Remainder theorem, and to also heavily use the fact that $a \equiv b \pmod m \implies a \equiv b \pmod d$, wherever d divides m.

   We have that $2^n + 5^n \equiv n \pmod{1000}$, so $2^n + 5^n \equiv n \pmod 8$ and $2^n + 5^n \equiv n \pmod{125}$. It is easy to check $n < 3$ don't work, so $n \geq 3$. Then, $2^n \equiv 0 \pmod 8$ and $5^n \equiv 0 \pmod{125}$, so we just have $5^n \equiv n \pmod 8$ and $2^n \equiv n \pmod{125}$. Let us consider both of these congruences separately.

   First, focus on $5^n \equiv n \pmod 8$. By Fermat's Little Theorem, we have $5^4 \equiv 1 \pmod 8$, so $5^5 \equiv 5 \pmod 8$. Note that this pattern holds, where $5^n \equiv 1 \pmod 8$ for even n, and $5^n \equiv 5 \pmod 8$ for odd n. So, the only solutions to this equation occur when $n \equiv 5 \pmod 8$, or $n = 8k + 5$.

   Now, we look at $2^n \equiv n \pmod{125}$. By what we stated above, this requires $2^n \equiv n \pmod{25}$ and $2^n \equiv n \pmod 5$. Plugging in $n = 8k + 5$, we get $2^{8k+5} \equiv 8k + 5 \pmod 5 \implies 2^{8k} \cdot 32 \equiv 8k \pmod 5$. By Fermat's Little Theorem, $2^4 \equiv 1 \implies 2^8 \equiv 1 \implies 2^{8k} \equiv 1 \pmod 5$. So we have $32 \equiv 2 \equiv 3k \pmod 5 \implies k = 5m + 4$.

   Then, $n = 8(5m+4)+5 = 40m+37$. Plugging in again, we get $2^{40m+37} \equiv 40m-3 \pmod{125} \implies 2^{40m+37} \equiv 40m - 3 \pmod{25}$. Euler's Totient Theorem tells us that $2^{20} \equiv 2^{40} \equiv 1 \pmod{25}$, so we get $2^{37} \equiv 2^{-3} \equiv 15m + 12 \pmod{25}$. Multiplying both sides by $2^3 = 8$, we have $1 \equiv 120m + 96 \equiv 20m + 21 \implies 20m \equiv 4 \pmod{25}$. This happens precisely when $m \equiv 4 \pmod 5$, aka $m = 5s + 4$. Plugging in for m, we have $m = 200s + 197$.

   Now, we are finally ready to plug n into the congruence modulo 125. As before, Euler's totient theorem tells us that $2^{100} \equiv 1 \pmod{25}$. So, we have $2^{200s+197} \equiv 2^{197} \equiv 2^{-3} \equiv 200s + 197 \equiv 75s + 72$. Multiplying both sides by 8 gives us $1 \equiv 600s + 576 \equiv 100s + 76 \implies -75 \equiv 50 \equiv 100s \pmod{125}$, which happens precisely when $s \equiv 3 \pmod 5$, or $s = 5x + 3$.

   Finally, plugging this in, we find that $n = 200(5x + 3) + 197 = 1000x + 600 + 197 = 1000x + 797$. So, the smallest positive value of n is 797.