P U M ∴ C

Number Theory A

1. Claim: $M = 2017, m = 3$.

   $m \geq 1 + \min\{1, 2, \ldots, 2017\} = 2$. However, for $m = 2$, then it comes from a triple with median 1, which requires another element less than or equal to 1, which cannot occur. Instead, we can explicitly describe a process to construct $m = 3$; for the first 1007 iterations, only choose from $\{3, 4, \ldots, 2017\}$. Then simply choose the three remaining values: 1, 2 and a value greater than 3.

   In order to obtain $M > 2017$ we would need to get an element in the list equal to 2017 and an element greater than 2017. However, this is impossible, since when there is an element equal to 2017 there cannot be one greater. Instead, we can explicitly describe a process to construct $M = 2017$; for the first 1007 iterations, only choose from $\{1, 2, \ldots, 2015\}$. Then simply choose the three remaining values: a value less than or equal to 2015, 2016 and 2017.

   $M - m = \boxed{2014}$.

   Problem written by Zack Stier

2. Assume all exponents considered are at least 1. For $n > 1$, a_n must have at least two distinct prime factors (so that a_{n-1} has one prime in common and a_{n+1} has another); it is clear that we can construct a sequence satisfying those requirements given $a_2 = cp^a q^b$ for p, q prime but c not necessarily prime, by choosing no other element in the sequence to share prime factors with c and by letting $p \mid a_1$ and $q \mid a_3$. We now simply wish to find the four smallest numbers of the form $cp^a q^b$. Looking at numbers of the form pq: $6 = 2 \cdot 3, 10 = 2 \cdot 5, 14 = 2 \cdot 7, 15 = 3 \cdot 5$. However, $12 = 2^2 \cdot 3$ is also of the desired form, but any other value of c gets $a_2 > 15$ (e.g., $pq = 6$, $c = 3 \implies a_2 = 18$. So, our desired value is $6 + 10 + 12 + 14 = \boxed{42}$.

   Problem written by Zack Stier

3. The content of a rectangular prisms with side lengths a, b, and c is

   $$(a + 2)(b + 2)(c + 2) - 8,$$

   so there is a rectangular prism with integer side lengths and content N iff $N + 8$ is a product of three integers, each of which is greater than 2. A bit of case work shows the least such N is $\boxed{55}$.

   Problem written by Matt Tyler

4. We see that b_n is $1 + lcm(1, 2, \ldots, n')$ where n' is the greatest integer less than n such that, for some prime $p \leq n$, $\log_p n' \in \mathbb{N}$. $36' = 32$ and $25' = 25$, so $\frac{1+\text{lcm}(1,2,\ldots,32)}{1+\text{lcm}(1,2,\ldots,25)} \approx \frac{\text{lcm}(1,2,\ldots,32)}{\text{lcm}(1,2,\ldots,25)} = 3 \cdot 29 \cdot 31 \cdot 2 = \boxed{5394}$.

   Problem written by Zack Stier

5. Let $x = n - 30$; then, we are looking at odd prime factors of $p(x)p(x + 60)$.

   First we look at $p(x) \pmod 3$. We find $p(x) \equiv x^2 - 1 \equiv 0 \iff x \not\equiv 0 \pmod 3$.

   Say now that $x \equiv 0 \pmod 3$, i.e. $x = 3y$. $p(x) = p(3y) \equiv y^4 + y^2 \pmod 5$. $y \equiv 0$ is clearly a solution; say temporarily that $y \not\equiv 0$, so $y^4 \equiv 1$; then for $5 \mid p(x)$, $y^2 \equiv -1 \pmod 5$, or $y \equiv 2, 3$.

   It takes a little more work to show that when $y \equiv \pm 1 \pmod 5$, $7 \mid p(x)p(x + 60)$, as it is not always the case that $7 \mid p(x)$ (as it was with 3 and 5). (In fact, we will show a stronger result – that 7 *always* divides the product.) Factor: $p(x) = (x^2 - 16)(x^2 + 10) \equiv (x^2 - 2)(x^2 - 4) \pmod 7$, and so $p(x + 60) \equiv ((x + 4)^2 - 2)((x + 4)^2 - 4)$. Now, consider the quadratic residues

modulo 7:

x	x^2	$x+4$	$(x+4)^2$
0	0	4	2
1	1	5	4
2	4	6	1
3	2	0	0
4	2	1	1
5	4	2	4
6	1	3	2

Note how each line has either a 2 or a 4 in the squared column; this means that 7 always divides the product $p(x)p(x+60)$ for any integer x.

Thus, we have $n \equiv 1, 2 \pmod 3 \implies a_n = 3$; $\frac{n}{5} \equiv 0, \pm 2 \pmod 5 \implies a_n = 5$; else $a_n = 7$. Summing gives $\boxed{7933}$.

Problem written by Zack Stier

6. Let's look at the period of powers of 2 modulo various odd primes p. If $p = 3$ then the period is 2, since $2^0 \equiv 2^2 \pmod 3$. Similarly, $p = 5$ has period 4, since $2^0 \equiv 2^4 \pmod 5$. Why is this useful? We know that if $N \cdot 2^n + 1 \equiv 0 \pmod p$ and p has period P_p then $N \cdot 2^{n+P_p} + 1 \equiv 0$ as well. Thus we want to "cover" the nonzero modulo-12 residue classes with various primes. This will give us what we want: if we can find a prime p for each m a non-multiple of 12 such that there is $0 < r < 12$ with $m \equiv r \pmod p$ then we will have succeeded. We use the following periods: $P_3 = 2, P_5 = 4, P_7 = 3, P_{13} = 12$. We start by placing the 3s to not cover the 0 residue:

0	1	2	3	4	5	6	7	8	9	10	11
	3		3		3		3		3		3

We now place the 5s as to be as non-redundant as possible, and also not cover the 0 residue:

0	1	2	3	4	5	6	7	8	9	10	11
	3	5	3		3	5	3		3	5	3

We now have choices to place the 7s; the 13 will then be placed in the last remaining spot:

0	1	2	3	4	5	6	7	8	9	10	11
	3	5	3		3	5	3		3	5	3
		7		13	7			7			7
	7			7			7	13		7	

(The latter two rows are the two possibilities.) Thus we must solve the linear systems (using the Chinese Remainder Theorem) and choose the viable value that is least:

$$\begin{aligned} 2N &\equiv -1 \pmod 3 \\ 4N &\equiv -1 \pmod 5 \\ 4N &\equiv -1 \pmod 7 \\ 16N &\equiv -1 \pmod{13} \\ \implies N &\equiv 901 \pmod{1365} \end{aligned} \qquad \begin{aligned} 2N &\equiv -1 \pmod 3 \\ 4N &\equiv -1 \pmod 5 \\ 2N &\equiv -1 \pmod 7 \\ 256N &\equiv -1 \pmod{13} \\ \implies N &\equiv 556 \pmod{1365} \end{aligned}$$

$N = \boxed{556}$ is the minimal value satisfying the desired property, and we are done.

Problem written by Zack Stier

7. Let $p = 17$. We work modulo p. Note that solutions come in pairs (x, y) and $(x, -y)$ (i.e. $(x, p-y)$), except for solutions $(x, 0)$. Thus, the number of solutions is even if and only if $x^3 + ax + b$ has an even number of distinct roots modulo p. To count such pairs (a, b) we employ complementary counting.

If x^3+ax+b has three distinct roots, it can be written in the form $(x-r)(x-s)(x+r+s)$ for $r \neq s$, $r \neq -r-s$ (so $s \neq -2r$), and $s \neq -r-s$ (so $r \neq -2s$). The number of such pairs (r,s) is p^2-3p+2. This is because there are p^2 pairs (r,s); p have $r=s$, p have $r=-2s$, p have $s=-2r$, and it is easy to see that there is no overlap, with the exception of $(0,0)$, which we counted thrice. Thus, p^2-3p+2 pairs (r,s) satisfy these conditions. Now, since we can permute the roots r, s, and $-r-s$ as we wish, the number of polynomials x^3+ax+b with three roots is $\frac{p^2-3p+2}{6}$.

If x^3+ax+b has exactly one root, it can be written as $(x-r)(x^2+rx+c)$ for some (r,c), where x^2+rx+c is irreducible. Thus, the number of such polynomials is the number of irreducible polynomials x^2+rx+c. The total number of quadratics modulo p is p^2, and the number of reducible quadratics is $p+\binom{p}{2}$ (because a reducible quadratic either has a double root — there are p of these — or has two distinct roots). This leaves $p^2-p-\binom{p}{2}=\frac{p(p-1)}{2}$ irreducible quadratics, and thus $\frac{p(p-1)}{2}$ polynomials of the form x^3+ax+b with exactly one root.

Thus, there are $\frac{p^2-3p+2}{6}+\frac{p^2-p}{2}$ such polynomials with an odd number of distinct roots, and since there are p^2 polynomials total (p possibilities for a and p possibilities for b), the number of polynomials with an even number of distinct roots, and thus the number of pairs (a,b) such that $y^2=x^3+ax+b$ has an even number of solutions modulo p, is

$$p^2-\left(\frac{p^2-3p+2}{6}+\frac{p^2-p}{2}\right)=\frac{2p^2+6p-2}{6}=\frac{p^2+3p-1}{3}.$$

Plugging in $p=17$, we obtain $\boxed{113}$ as our answer.

Problem written by Eric Neyman

8. Algebraic manipulation reduces this to minimizing $\sum_{x=a}^{a+99}\gcd(x,400)$ for $a \in \mathbb{N}$ (by playing with the variables and noting periodicity and symmetry of gcd about 0). We claim this occurs at $a=1$. Set $k=100$ and $n=400$. We now solve this problem in generality.

Lemma: Let n be a positive integer and let S be a finite multiset of factors of n. For each $d \mid n$, let $m_d(S)$ be the number of multiples of d in S. Then

$$\sum_{k \in S} k = \sum_{d \mid n} m_d(S)\phi(d).$$

Proof: This is a simple induction on the number of elements of S. The theorem is clear for $|S|=0$; suppose it holds for $|S|=r$. Now let S have $r+1$ elements and choose $k \in S$. Let S' be S with one fewer copy of k; the theorem holds for S'. Adding k to S' increments the left-hand sum by k and the right-hand sum by $\sum_{d \mid k}\phi(d)$, since $m_d(S)=m_d(S')+1$ for $d \mid k$ and $m_d(S)=m_d(S')$ for all other d. But $\sum_{d \mid k}\phi(d)=k$, so the theorem holds for S. This completes our induction.

For n implicit, define the multiset $S_{a,k}=\{\gcd(x,n) \mid x \in \{a,a+1,\ldots,a+k-1\}\}$. Observe that for all $d \mid n$, holding k constant, $m_d(S_{a,k})$ is minimal for $a=1$. It follows from the Lemma that $\sum_{x=a}^{a+k-1}\gcd(x,n)$ is minimized for $a=1$, as desired.

Going back to the problem, we thus find that the minimum value occurs at $M=101$; a consequence is that 0 is also a minimum; and thus 2000 too is a minimum. Computation gives that the sum there is equal to $\boxed{680}$.

Problem written by Eric Neyman and Zack Stier

If you believe that any of these answers is incorrect, or that a problem had multiple reasonable interpretations or was incorrectly stated, you may appeal at http://tinyurl.com/PUMaCappeal2017. All appeals must be in by 1 PM to be considered.