Number Theory A Solutions

1. Find the integer x for which $135^3 + 138^3 = x^3 - 1$.

   Proposed by Sunay Joshi

   Answer: $\boxed{172}$

   We claim that $x = 172$.

   First, we show that x lies in the interval $[138, 184]$. That the lower bound holds is clear. To see the upper bound, note that

$$x^3 = 135^3 + 138^3 + 1 \leq 2 \cdot 138^3 \to x \leq \sqrt[3]{2} \cdot 138$$

   Let $\sqrt[3]{2} = 1 + h$; then $(1+h)^3 = 2$. By Bernoulli's Inequality, $1 + 3h \leq (1+h)^3$, implying that $h \leq \frac{1}{3}$ and hence $\sqrt[3]{2} \leq \frac{4}{3}$. Our upper bound is therefore $x \leq \frac{4}{3} \cdot 138 = 184$, as claimed.

   Next, we consider the equation $x^3 = 135^3 + 138^3 + 1$ modulo p for $p = 5, 11$. We choose these values of p because for $p \not\equiv 1 \pmod 3$, the cubing map $x \mapsto x^3$ is a bijection from $\mathbb{Z}/p\mathbb{Z}$ to itself. For $p = 5$, we compute $x^3 \equiv 0^3 + 3^3 + 1 \equiv 3 \pmod 5$, hence $x \equiv 2 \pmod 5$. For $p = 11$, we compute $x^3 \equiv 3^3 + 6^3 + 1 \equiv 2 \pmod{11}$, hence $x \equiv 7 \pmod{11}$. By the Chinese Remainder Theorem, it follows that $x \equiv 7 \pmod{55}$, and it is easy to see that the unique number of the form $55k + 7$ in the interval $[138, 184]$ is 172.

   Remark: This identity was discovered by Ramanujan.

2. A number is called *good* if it can be written as the sum of the squares of three consecutive positive integers. A number is called *excellent* if it can be written as the sum of the squares of four consecutive positive integers. (For instance, $14 = 1^2 + 2^2 + 3^2$ is good and $30 = 1^2 + 2^2 + 3^2 + 4^2$ is excellent.) A good number G is called *splendid* if there exists an excellent number E such that $3G - E = 2025$. If the sum of all splendid numbers is S, find the remainder when S is divided by 1000.

   Proposed by Sunay Joshi

   Answer: $\boxed{447}$

   Any good number can be written as $(n-1)^2 + n^2 + (n+1)^2 = 3n^2 + 2$ for some $n \geq 2$. Similarly any excellent number can be written as $(m-1)^2 + m^2 + (m+1)^2 + (m+2)^2 = (2m+1)^2 + 5$ for some $m \geq 2$. Therefore, a good number $3n^2 + 2$ (with $n \geq 2$) is excellent iff there exists $m \geq 2$ such that $3(3n^2 + 2) - ((2m+1)^2 + 5) = 2025$. Rearranging, this is equivalent to $9n^2 - (2m+1)^2 = 2024$. By the difference of squares, this becomes $(3n - (2m+1))(3n + (2m+1)) = 2^3 \cdot 11 \cdot 23$. Since the two factors add to the even number $6n$, it is clear that each must be even. The possible factor pairs (x, y) with $x < y$ and $x, y > 0$ are thus $(2, 4 \cdot 11 \cdot 23)$, $(4, 2 \cdot 11 \cdot 23)$, $(2 \cdot 11, 4 \cdot 23)$, and $(4 \cdot 11, 2 \cdot 23)$. These correspond to $(n, m) = (169, 252), (85, 125), (19, 17), (15, 0)$. Since we require $m, n \geq 2$, only the first three pairs are valid solutions. It follows that $n \in \{169, 85, 19\}$, so the set of splendid numbers is $\{3 \cdot 169^2 + 2, 3 \cdot 85^2 + 2, 3 \cdot 19^2 + 2\}$. Thus $S = (3 \cdot 169^2 + 2) + (3 \cdot 85^2 + 2) + (3 \cdot 19^2 + 2)$, which is congruent to $447 \pmod{1000}$.

3. Call an arrangement of n not necessarily distinct nonnegative integers in a circle *wholesome* when, for any subset of the integers such that no pair of them is adjacent in the circle, their average is an integer. Over all wholesome arrangements of n integers where at least two of them are distinct, let $M(n)$ denote the smallest possible value for the maximum of the integers in the arrangement. What is the largest integer $n < 2023$ such that $M(n+1)$ is strictly greater than $M(n)$?

Proposed by Austen Mazenko

Answer: $\boxed{2018}$

The idea is as follows: consider any $k \leq \lfloor (n-1)/2 \rfloor$ not pairwise adjacent integers in a wholesome arrangement. By Pigeonhole, at least one of them can be replaced by one of its neighbors to get another subset such that no two are pairwise adjacent; this integer and its neighbor are thus equivalent modulo k, and by symmetry around the circle, this means that all of the intgers are congruent modulo k for all such k. If n is odd, this covers all possible integers; letting them all be 0 except for one which is $\text{lcm}(1, 2, ..., \lfloor (n-1)/2 \rfloor)$ is therefore optimal, and $M(n)$ equals this least common multiple in such cases. If n is even, we have to consider the two disjoint subsets consisting of $n/2$ of the integers with no two adjacent. In this case, their sum must be a multiple of $n/2$, but evidently generalizing the previous construction such that the integers in the circle are alternating with values 0 and $\text{lcm}(1, 2, ..., \lfloor (n-1)/2 \rfloor)$ shows $M(2m) = M(2m-1)$ (since $M(2m) \geq M(2m-1)$ obviously holds by just ignoring one of the extra integers, and we just showed equality is achievable). Now, $M(2m+1) = M(2m)$ whenever $\text{lcm}(1, 2, ..., m) = \text{lcm}(1, 2, ..., m-1)$. Thus the desired condition holds precisely when $m \nmid \text{lcm}(1, 2, ..., m-1)$, meaning m is a prime power. Specifically, we want to find the largest m such that $2m < 2023$ and m is a prime power. A quick check shows that $m = 1009$ is prime, so our answer is 2018.

4. What is the smallest possible sum of six distinct positive integers for which the sum of any five of them is prime?

Proposed by Austen Mazenko

Answer: $\boxed{74}$

The smallest possible sum is 74, achieved for the integers $1, 3, 7, 15, 21, 27$.

Consider the sum of the smallest five integers, which is 47 in this case. Suppose there was a more optimal solution with a smallest sum larger than 47. Now, the five other sums must be distinct prime numbers greater than this value, meaning the sum of the largest five integers is at least six primes greater than 47; in particular, it's at least 73, meaning the sum of all six integers is at least 74 as claimed.

Now, suppose the sum of the smallest five integers is $p < 47$, and let the integers be $a_1, a_2, ..., a_6$ in increasing order. Thus, $a_1+a_2+a_3+a_4+a_5 = p$, and since subbing out any of the summands for a_6 gives another prime sum, $p + a_6 - a_i$ is prime for $1 \leq i \leq 5$. Since $p \neq 2$, it's odd, so $a_6 - a_i$ is even meaning all the a_i have the same parity; hence, they're all odd. Thus, $p \geq 1 + 3 + 5 + 7 + 9 = 25$, so we need to check $p = 29, 31, 37, 41, 43$. Define $p_i := p + a_6 - a_i$, so p_i is some prime larger than p. Summing the equation $a_6 - a_i = p_i - p$ for $1 \leq i \leq 5$ gives $5a_6 - p = \sum_{i=1}^{5}(p_i - p)$, so $a_6 = \frac{p+\sum_{i=1}^{5}(p_i-p)}{5}$. Since the a_i are increasing, p_1 is the largest difference, and thus $a_6 = a_1 + p_1 - p > p_1 - p$. For a fixed p_1, we maximize a_6 by taking p_2, p_3, p_4, p_5 to be the four primes just less than p_1. Then, we need $\frac{p+\sum_{i=1}^{5}(p_i-p)}{5} > p_1 - p$, which is equivalent to

$$\frac{p + \sum_{i=1}^{5}(p_i - p_1 + p_1 - p)}{5} > p_1 - p \Leftrightarrow p > \sum_{i=1}^{5}(p_1 - p_i) \quad \bigstar.$$

Looking at differences of consecutive primes at least 29 and at most 73, namely $2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2$, we see that the minimal possible value for $\sum_{i=1}^{5}(p_1 - p_i)$ is $2+(2+4)+(2+4+6)+(2+4+6+2) = 34$, so $p = 29, 31$ do not work. Finally, since $p + \sum_{i=1}^{5}(p_i - p)$ must be a multiple of 5, simply checking $p = 37, 41, 43$ gives the result. Specifically, if $p = 43$, then $p_1 = 67$ or 71. To accommodate the modulo 5 constraint, the only values for the other p_i are $47, 53, 59, 61$ and $47, 53, 59, 67$, respectively, but these do not satisfy $\bigstar$. If $p = 41$, then to accommodate the modulo 5 constraint either $p_1 = 71$ in which case the other primes must be $43, 47, 61, 67$ or $47, 53, 61, 67$, neither of which satisfy ★, or $p_1 = 67$ so the other primes are $43, 47, 53, 59$ which also fail. Finally, if $p = 37$, then in order for ★ to be satisfied, we must have $p_1 = 71$ and the other primes are $53, 59, 61, 67$, but this violates the modulo 5 condition, so we may conclude.

5. You play a game where you and an adversarial opponent take turns writing down positive integers on a chalkboard; the only condition is that, if m and n are written consecutively on the board, $\gcd(m, n)$ must be squarefree. If your objective is to make sure as many integers as possible that are strictly less than 404 end up on the board (and your opponent is trying to minimize this quantity), how many more such integers can you guarantee will eventually be written on the board if you get to move first as opposed to when your opponent gets to move first?

   Proposed by Austen Mazenko

   Answer: $\boxed{94}$

   Note that you can always write squarefree numbers on the board, and thus regardless of whether you move first or second, you can guarantee all squarefree numbers less than 404 get written. Now, if you go second, your opponent can guarantee that you can *only* write squarefree numbers by simply writing multiples of $2^2 \cdot 3^2 \cdot 5^2 \cdots 401^2$ on the board. Thus, it suffices to find the maximum number of non-squarefree numbers you can guarantee get written on the board if you go first. For any prime p, if you ever write a number m such that $p^2 \nmid m$, then your opponent can continually choose multiples of p^2 that are greater than 404 which prevents you from writing any more multiples of p^2. Note also that writing any number greater than 404 functionally just stalls the game by a round and cannot give you any advantage. Thus, to play optimally, you should thus write all multiples of $2^2 \cdot 3^2 = 36$ less than 404, after which you should write everything expressible as 4 times a number with no odd divisors that are the squares of a prime, then finally squarefree integers. Tallying, we see there are 11 multiples of 36. Then, looking at 4 times an odd number, we see there are 26 possibilities (odd primes and 1) plus 9 possibilities (3 times an odd prime) plus 5 possibilities (5 times an odd prime) plus 2 possibilities (7 times an odd prime). Next, looking at 8 times an odd number, we see there are 15 possibilities (odd primes and 1) plus 4 possibilities (3 times an odd prime) plus 1 possibility (35); next, looking at 16 times an odd number, we see there are 9 possibilities plus 2 possibilities; next, looking at 32 times an odd number, we see that there are 5 possibilities, then for 64 there are 3 possibilities, for 128 there are 2, and for 256 there is just the 1. In total, we get $11 + 26 + 9 + 5 + 2 + 15 + 4 + 1 + 9 + 2 + 5 + 3 + 2 = 94$.

6. How many positive integers $n \leq \operatorname{lcm}(1, 2, \ldots, 100)$ have the property that n gives different remainders when divided by each of $2, 3, \ldots, 100$?

   Proposed by Daniel Zhu

   Answer: $\boxed{1025}$

   Observe that, of the remainders $0, 1, ..., 99$, exactly one will not be used. Moreover, notice that choosing a remainder for each integer $2, 3, ..., 100$ uniquely determines $n \leq \operatorname{lcm}(1, 2, ..., 100)$ by Chinese remainder theorem (CRT).

   If 0 isn't the excluded remainder, let a be the unique number that n leaves a remainder of 0 divided by, so $a|n$. Clearly, a must be prime, as otherwise n would also leave a remainder when divided by a factor of a greater than 1. Assume for now that $a > 2$. Considering the remainders of n modulo $2, 3, 4, ..., a-1$, we note that they are fixed; because 0 is already used modulo a, the only possible remainder modulo 2 is 1; since 0 and 1 are already used, the only possible remainder modulo 3 is 2, and so on. Looking at $n \pmod{a+1}$, because a is prime $a+1$ isn't, so by Chinese remainder theorem n must be -1 modulo the factors of $a+1$ meaning $n \equiv a \pmod{a+1}$. Now, if $2a \leq 100$, because $a|n$ we must have that n modulo $2a$ is either 0 or a, contradiction as both of these remainders have already used. Thus, a must be a prime between 50 and 100.

Now, suppose that n is odd, meaning $n \equiv 1 \pmod 2$. We claim that $n \equiv k-1 \pmod k$ for all $2 \le k \le 100$ such that k is not a prime between 50 and 100. This follows by strong induction. The base case $k=2$ holds by assumption. Then, for higher k, if k is composite then by Chinese remainder theorem on its factors and the inductive hypothesis we have $n \equiv -1 \pmod k$. Contrarily, if k is prime, by induction the possible unused remainders are 0 and $k-1$, but we showed earlier that if 0 is a remainder it must be mod 2 or a prime greater than 50, so it can't be the remainder of n modulo k. This establishes the claim. Next, let $p_1 < p_2 < \cdots < p_{10}$ denote the primes between 50 and 100. We thus want to find the number of ways to allocate all but one of the elements in the set $\{0\} \cup \{p_1-1, ..., p_{10}-1\}$ as remainders of n modulo the elements in $\{p_1, ..., p_{10}\}$. Assigning the remainder to p_1 first, then p_2, etc., up to p_{10}, note there are two choices at each step, for a total of 2^{10} distinct allocations.

The remaining case is that n is even; we claim this forces $n \equiv k-2 \pmod k$ for all $2 \le k \le 100$. But, we see by induction the even remainders are fixed, and then by induction again for odds k we see that $k-1, k-2$ are the only possible remainders, but $k-1$ is the remainder modulo the even number $k+1$, so it must be $k-2$. Thus, this contributes one additional possible value for n, making our answer $2^{10}+1 = 1025$.

7. Define $f(n)$ to be the smallest integer such that for every positive divisor $d|n$, either $n|d^d$ or $d^d|n^{f(n)}$. How many positive integers $b < 1000$ which are not squarefree satisfy the equation $f(2023) \cdot f(b) = f(2023b)$?

Austen Mazenko

Answer: $\boxed{5}$

The crux of the problem is the following claim:

Lemma 1: Let $n = \prod_i p_i^{e_i}$ be the prime factorization of n. Then $f(n) = \frac{n}{\min_i p_i^{e_i}}$.

Proof: To prove it, we first show that this value is necessary. Let $d = \frac{n}{\min_i p_i^{e_i}} | n$. Denoting $k := \arg\min_i p_i^{e_i}$, trivially $p_k | n$ but $d = \frac{n}{p_k^{e_k}} \implies p_k \nmid d \implies p_k \nmid d^d$, so $n \nmid d^d$.

Because $d^d | n^{f(n)}$, $\nu_{p_i}(d^d) \le \nu_{p_i}(n^{f(n)})$ which, for $i \ne k$, is $e_i \cdot \frac{n}{p_k^{e_k}} \le e_i \cdot f(n)$, so $\frac{n}{\min_i p_i^{e_i}} \le f(n)$ as claimed.

To see that it's sufficient, we split into cases to show that $d|n$ implies $n|d^d$ or $d^d | n^{\frac{n}{\min_i p_i^{e_i}}}$. First, suppose there exists some prime $p_j | n$ that doesn't divide d. Denote $d_j := \frac{n}{p_j^{e_j}}$. Then, $d | d_j \implies d^d | d_j^{d_j}$, and $d_j^{d_j} | n^{\frac{n}{\min_i p_i^{e_i}}}$ because for any $\ell \ne j$,

$$\nu_{p_\ell}(d_j^{d_j}) = e_\ell \cdot d_j \le e_\ell \cdot \frac{n}{\min_i p_i^{e_i}} = \nu_{p_\ell}\left(n^{\frac{n}{\min_i p_i^{e_i}}}\right).$$

It remains to address the case where d possesses the same prime factors as n. Write $d = \prod_i p_i^{a_i}$ with $1 \le a_i \le e_i$ for each i, and consider when $n|d^d$. It holds whenever for each ℓ we have $\nu_{p_\ell}(n) = e_\ell \le a_\ell \cdot \prod_i p_i^{a_i} = \nu_{p_\ell}(d^d)$. Next, suppose there exists some k such that $e_k > a_k \cdot \prod_i p_i^{a_i}$. It suffices to show that in this case we have $d^d | n^{\frac{n}{\min_i p_i^{e_i}}}$, which by looking at valuations is the same as $a_\ell \cdot \prod_i p_i^{a_i} \le e_\ell \cdot \frac{n}{\min_i p_i^{e_i}}$ for each ℓ. By assumption, $\prod_i p_i^{a_i} < \max_i \frac{e_i}{a_i}$, so $\frac{a_\ell}{e_\ell} \cdot \prod_i p_i^{a_i} < \frac{a_\ell}{e_\ell} \cdot \frac{e_k}{a_k} \le \frac{n}{\min_i p_i^{e_i}}$ which implies the result. To see why this last inequality holds, note that if n is a prime power then we have equality as $\ell = k$. Otherwise,

$$\frac{n}{\min_i p_i^{e_i}} \ge \sqrt{n} = \prod_i p_i^{e_i/2} \ge 2^{1/2} \cdot 2^{e_k/2} \ge e_k \ge \frac{e_k}{a_k} \cdot \frac{a_\ell}{e_\ell},$$

which is precisely the claimed bound. □

To finish the problem, for simplicity denote $g(n) := \frac{n}{f(n)}$, so $g(n)$ is the smallest prime power appearing in the prime factorization of n. Notice $f(m) \cdot f(n) = f(mn) \iff \frac{m}{g(m)} \cdot \frac{n}{g(n)} = \frac{mn}{g(mn)} \iff g(mn) = g(m) \cdot g(n)$, so it suffices to solve $g(2023b) = g(2023) \cdot g(b) = 7g(b)$. Now, $g(b)$ and $g(2023b)$ are both prime powers, and thus must both be powers of 7. If $49|g(b)$, then either $g(b) = 49$ or 343 because otherwise $g(b)$ must have some other prime power factor, but this would have to exceed 49, so $b > 49^2 > 1000$. However, if $b \geq 49$ is a power of 7 then $g(2023b)$ is not, contradiction. Thus, $g(b) = 7$, forcing $g(2023b) = 49$. Writing $b = 7a$ for some $7 \nmid a$, we see that any prime power dividing a other than 17 must be at least 49. If $17|a$, then either $17^2|a \implies b > 1000$ or a is $7 \cdot 17\cdot$ some prime power greater than 49, which again forces $b > 1000$. Thus, the only possibilities are a is a prime power greater than 49 (and with exponent greater than 1) such that $7a < 1000$. Tabulating, we see the only possibilities are $b = 7 \cdot 64, 7 \cdot 81, 7 \cdot 121, 7 \cdot 125, 7 \cdot 128$, giving a final answer of 5.

8. Let $S_0 = 0, S_1 = 1$, and for $n \geq 2$ let $S_n = S_{n-1} + 5S_{n-2}$. What is the sum of the five smallest primes p such that $p \mid S_{p-1}$?

Proposed by Owen Yang

Answer: $\boxed{185}$

Claim 1: $S_n = \frac{1}{\sqrt{21}}\left(\left(\frac{1+\sqrt{21}}{2}\right)^n - \left(\frac{1-\sqrt{21}}{2}\right)^n\right)$

Proof: We proceed by strong induction. Our base cases are $S_0 = 0$ and $S_1 = 1$ which can be easily checked to work. For the inductive step, we have that

$$\left(\frac{1+\sqrt{21}}{2}\right)^2 = \frac{22+2\sqrt{21}}{4} = \frac{11+\sqrt{21}}{2} = \frac{1+\sqrt{21}}{2} + 5$$

and similarly

$$\left(\frac{1-\sqrt{21}}{2}\right)^2 = \frac{22-2\sqrt{21}}{4} = \frac{11-\sqrt{21}}{2} = \frac{1-\sqrt{21}}{2} + 5$$

so if the formulas work for S_{n-1} and S_n then we have

$$S_{n+1} = S_n + 5S_{n-1} = \frac{1}{\sqrt{21}}\left(\left(\frac{1+\sqrt{21}}{2}\right)^n + 5\left(\frac{1+\sqrt{21}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{21}}{2}\right)^n - 5\left(\frac{1-\sqrt{21}}{2}\right)^{n-1}\right)$$

$$= \frac{1}{\sqrt{21}}\left(\left(\frac{1+\sqrt{21}}{2}\right)^n - \left(\frac{1-\sqrt{21}}{2}\right)^n\right)$$

as desired.

Claim 2:

$$S_n = \frac{\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 21^k}{2^{n-1}}$$

Proof: We compute the coefficients in the binomial expansions of the formula from Claim 1. We have

$$S_n = \frac{1}{\sqrt{21}}\left(\frac{\sum_{i=0}^n \binom{n}{i}\sqrt{21}^i - \sum_{i=0}^n \binom{n}{i}(-\sqrt{21})^i}{2^n}\right)$$

for which the coefficients cancel when i is even and are doubled when i is odd. Re-indexing with $i = 2k+1$, we find that

$$S_n = \frac{1}{\sqrt{21}}\left(\frac{\sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor} 2\binom{n}{2k+1}21^k\sqrt{21}}{2^n}\right) = \frac{\sum_{k=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2k+1}21^k}{2^{n-1}}$$

as desired.

Claim 3: For prime $p \neq 2$, we have that $S_p \equiv 21^{\frac{p-1}{2}} \bmod p$ and $S_{p+1} \equiv 2^{-1}(1+21^{\frac{p-1}{2}}) \bmod p$.

Proof: Note that since p is prime, p divides all binomial coefficients $\binom{n}{k}$ with $n = p$ except for $k = 0$ and $k = p$. Then since the sum formula from Claim 2 contains only coefficients with k odd, the only one not divisible by p is the last one, $\binom{p}{p} = 1$ (here we use the fact that p is odd). Then we find that

$$2^{p-1}S_p = \sum_{k=0}^{\lfloor\frac{p-1}{2}\rfloor}\binom{p}{2k+1}21^k \equiv 21^{\frac{p-1}{2}} \pmod p$$

and since $2^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem, we obtain that $S_p \equiv 21^{\frac{p-1}{2}} \pmod p$ as desired. Similarly, for $n = p+1$ we know that p divides all coefficients between $k = 2$ and $p-1$, inclusive. The odd values of k are 1 and p, so

$$2^pS_{p+1} = \sum_{k=0}^{\lfloor\frac{p}{2}\rfloor}\binom{p+1}{2k+1}21^k \equiv \binom{p+1}{1}21^0 + \binom{p+1}{p}21^{\frac{p-1}{2}} \pmod p$$

$$\equiv (p+1)(1+21^{\frac{p-1}{2}}) \pmod p \equiv 1 + 21^{\frac{p-1}{2}} \pmod p$$

so that

$$2^pS_{p+1} \equiv 2S_{p+1} \equiv 1 + 21^{\frac{p-1}{2}} \pmod p$$

$$\implies S_{p+1} \equiv 2^{-1}(1+21^{\frac{p-1}{2}}) \pmod p$$

Claim 4: For prime $p \neq 2, 3, 5, 7$, $p \mid S_{p-1} \iff \left(\frac{21}{p}\right) = 1$.

Proof: First note that $S_{p+1} \equiv S_p + 5S_{p-1} \pmod p \implies S_{p-1} \equiv 5^{-1}(S_{p+1} - S_p)$. Now if $\left(\frac{21}{p}\right) = 1$ then $21^{\frac{p-1}{2}} \equiv 1 \pmod p$ and from Claim 3 we calculate that $S_p \equiv S_{p+1} \equiv 1 \pmod p$. Then $S_{p-1} \equiv 5^{-1}(S_{p+1} - S_p) \equiv 0 \pmod p$ as desired. For the inverse, since $p \nmid 21$ we have $\left(\frac{21}{p}\right) = -1$, so that $21^{\frac{p-1}{2}} \equiv -1 \pmod p$. In particular, $S_p \equiv -1 \pmod p$ and $S_{p+1} \equiv 0 \pmod p$, so $S_{p-1} \equiv 5^{-1} \not\equiv 0 \pmod p$.

Now we can explicitly check the edge cases: we have $2 \nmid S_1 = 1$, $3 \nmid S_2 = 1$, $5 \nmid S_4 = 11$, and $7 \nmid S_6 = 86$. Therefore, we just need to find the smallest five primes such that $\left(\frac{21}{p}\right) = 1$. By quadratic reciprocity, we have that $\left(\frac{21}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{(p-1)}{2}(1+3)}\left(\frac{p}{3}\right)\left(\frac{p}{7}\right) = \left(\frac{p}{3}\right)\left(\frac{p}{7}\right)$. Then p must be either a residue or non-residue in both moduli, i.e. both $p \equiv 1 \pmod 3$ and $p \equiv 1, 2, \text{ or } 4 \pmod 7$, or both $p \equiv 2 \pmod 3$ and $p \equiv 3, 5, \text{ or } 6 \pmod 7$. The smallest five primes with this property are $17, 37, 41, 43$, and 47, so our final answer is $17+37+41+43+47 = \boxed{185}$.