MathCastle

Number Theory Open

Individual Round

10 questions • 30 minutes

Name _____

School _____

INSTRUCTIONS

1. This round has 10 problems. You have 30 minutes.
2. No calculators. Write your final answer in the blank beside each problem.
3. Answers must be simplified, with fractions in lowest terms.

Total Correct	Scorer's Initials

DO NOT BEGIN UNTIL YOU ARE TOLD TO DO SO.

1. Adding 105 to a power of two sometimes produces a perfect square: for example $2^4 + 105 = 121 = 11^2$. Find the sum of $x + y$ over all ordered pairs (x, y) of positive integers satisfying $2^x + 105 = y^2$. 1. _____

---

2. The number 9797 is the product of the two primes 97 and 101. Find the remainder when $96! = 1 \cdot 2 \cdot 3 \cdots 96$ is divided by 9797. (Give the remainder as an integer from 0 to 9796.) 2. _____

---

3. For how many ordered pairs (a, b) of integers with $1 \le a \le 100$ and $1 \le b \le 100$ is a^b a perfect square and, at the same time, b^a a perfect cube? (Here 1 counts as both a perfect square and a perfect cube.) 3. _____

---

4. A lock code is a seven-digit number in which each of the digits $1, 2, 3, 4, 5, 6, 7$ appears exactly once, so there are 5040 possible codes. How many of these codes, read as ordinary base-ten numbers, are divisible by 7? 4. _____

---

5. How many ordered pairs (x, y) of integers with $0 \le x \le 999$ and $0 \le y \le 999$ satisfy $xy \equiv x + y - 1 \pmod{1000}$? 5. _____

---

6. When a positive integer n is divided by an integer $k \ge 2$, write $n = qk + r$ with quotient q and remainder r, $0 \le r < k$. For example, $n = 10$ divided by $k = 4$ gives $q = r = 2$. For how many integers n with $1 \le n \le 1000$ is there *exactly one* integer $k \ge 2$ for which the remainder equals the quotient? 6. _____

---

7. Start with the number 1. At each step you may replace the current number x by $2x$, by $3x$, or by $x+47$. For example, $1 \to 3 \to 50 \to 100$ reaches 100 in three steps. How many integers n with $1 \le n \le 1000$ can be reached after some number of steps? (Zero steps are allowed, so 1 counts.) 7. _____

---

8. Call a positive integer n *complete* if every integer is congruent modulo n to some number of the form $x^2 + 2y^2$ with x and y integers. (For instance, $n = 1$ is complete.) How many of the integers $1, 2, 3, \ldots, 1000$ are complete? 8. _____

---

9. Find the sum of $m+n$ over all ordered pairs (m, n) of positive integers for which both $m^2 + 7n$ and $n^2 + 7m$ are perfect squares. 9. _____

---

10. Define a map T on the set $\{0, 1, 2, \ldots, 9999\}$ by letting $T(x)$ be the remainder when $3x+1$ is divided by 10000. This map is a permutation of the set, so repeatedly applying T to any starting element eventually returns to it, and the set splits into disjoint cycles. (A fixed point counts as a cycle of length 1.) How many cycles are there?

10. _____

Answer Key — Number Theory Open Practice Contest 2

1. 61
2. 4364
3. 1948
4. 720
5. 8500
6. 179
7. 460
8. 814
9. 4668
10. 34

Solutions — Number Theory Open Practice Contest 2

1. Answer: 61. **The idea.** If x is even, 2^x is a square and the equation is a difference of two squares, which factors. If x is odd, look modulo 5: the left side can never be a square.

Work it out. *Odd x.* The powers of 2 modulo 5 cycle $2, 4, 3, 1$, so for odd x we have $2^x \equiv 2$ or $3 \pmod 5$. Since $105 \equiv 0 \pmod 5$, $y^2 \equiv 2$ or $3 \pmod 5$. But squares modulo 5 are only $0, 1, 4$. So x is even.

Even $x = 2m$. Then $y^2 - (2^m)^2 = 105$, i.e. $(y - 2^m)(y + 2^m) = 105 = 3 \cdot 5 \cdot 7$. Both factors are positive, and their difference is 2^{m+1}. The factor pairs of 105 are $(1, 105), (3, 35), (5, 21), (7, 15)$, with differences $104, 32, 16, 8$. Only powers of two are allowed: 104 is not one, while $32 = 2^5$, $16 = 2^4$, $8 = 2^3$ are. These give $m = 4, 3, 2$ and $y = 19, 13, 11$ (half the sum of the factors). So the solutions are $(x, y) = (8, 19), (6, 13), (4, 11)$.

The requested sum is $27 + 19 + 15 = 61$.

Check. $2^8 + 105 = 361 = 19^2$, $2^6 + 105 = 169 = 13^2$, $2^4 + 105 = 121 = 11^2$. And for odd x, e.g. $2^1 + 105 = 107$, $2^3 + 105 = 113$, $2^5 + 105 = 137$, $2^7 + 105 = 233$: none are squares, as the mod 5 argument says.

2. Answer: 4364. **The idea.** By the Chinese remainder theorem it is enough to know 96! modulo 97 and modulo 101. Wilson's theorem, $(p-1)! \equiv -1 \pmod p$ for a prime p, gives both: $96! = (97-1)!$ directly, and $96!$ is $100! = (101-1)!$ with its last four factors removed, which are $\equiv -4, -3, -2, -1 \pmod{101}$.

Work it out. *Wilson's theorem.* Modulo a prime p, each of $1, 2, \ldots, p-1$ has an inverse in the same list, and a is its own inverse only when $a^2 \equiv 1$, i.e. $p \mid (a-1)(a+1)$, i.e. $a = 1$ or $a = p-1$. Pairing every other factor with its inverse, $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod p$.

Modulo 97. $96! \equiv -1 \equiv 96 \pmod{97}$.

Modulo 101. $-1 \equiv 100! = 96! \cdot 97 \cdot 98 \cdot 99 \cdot 100 \equiv 96! \cdot (-4)(-3)(-2)(-1) = 24 \cdot 96! \pmod{101}$. Since $24 \cdot 80 = 1920 = 19 \cdot 101 + 1$, the inverse of 24 is 80, so $96! \equiv -80 \equiv 21 \pmod{101}$.

Combine. Write $x = 97t - 1$ (this is $\equiv -1 \pmod{97}$). We need $97t - 1 \equiv 21 \pmod{101}$, i.e. $-4t \equiv 22$, i.e. $4t \equiv -22 \equiv 79 \equiv 180 \pmod{101}$, so $t \equiv 45 \pmod{101}$ (as $\gcd(4, 101) = 1$). Then $x = 97 \cdot 45 - 1 = 4364$, which lies in $0, \ldots, 9796$.

So the remainder is 4364.

Check. $4364 = 97 \cdot 45 - 1 \equiv -1 \pmod{97}$, and $4364 = 101 \cdot 43 + 21 \equiv 21 \pmod{101}$. Also $24 \cdot 21 = 504 = 5 \cdot 101 - 1 \equiv -1 \pmod{101}$, consistent with $24 \cdot 96! \equiv -1$. Wilson itself is easy to test on a small prime: $6! = 720 = 7 \cdot 103 - 1$.

3. Answer: 1948. **The idea.** Decide each condition separately by exponents: a^b is a square exactly when b is even or a itself is a square, and b^a is a cube exactly when $3 \mid a$ or b itself is a cube. Both conditions then depend on which of two properties a has, so sort a into four classes.

Work it out. Write $a = \prod p^{e_p}$. Then a^b is a square iff every be_p is even, iff b is even or every e_p is even (i.e. a is a square). Similarly $b^a = \prod q^{af_q}$ is a cube iff every af_q is divisible by 3, iff $3 \mid a$ or b is a cube.

Among $1, \ldots, 100$ there are 10 squares, 33 multiples of 3, and 3 numbers that are both $(9, 36, 81)$.

a a square and a multiple of 3 (3 values): every b works, $3 \cdot 100 = 300$.

a a square, not a multiple of 3 (7 values): need b a cube: $b \in \{1, 8, 27, 64\}$, $7 \cdot 4 = 28$.

a a multiple of 3*, not a square* (30 values): need b even: $30 \cdot 50 = 1500$.

neither (60 values): need b even and a cube: $b \in \{8, 64\}$, $60 \cdot 2 = 120$.

Total $300 + 28 + 1500 + 120 = 1948$.

Check. $(a, b) = (2, 8)$: $2^8 = 16^2$ and $8^2 = 4^3$. $(a, b) = (6, 5)$: 6^5 is not a square (odd exponent on 2), correctly excluded since 6 is not a square and 5 is odd. The class sizes add to $3 + 7 + 30 + 60 = 100$.

4. Answer: 720**. The idea.** Look for a bijection on the codes that raises the remainder modulo 7 by exactly 1. Then all seven remainders occur equally often. The map is: replace every digit d by $d + 1$, except that 7 becomes 1.

Work it out. The map $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 7 \to 1$ permutes the digit set, so it sends codes to codes, and it is invertible (shift down), so it is a bijection on the 5040 codes.

Modulo 7 the digit 7 is 0, so in every position the new digit is congruent to the old digit plus 1 (including $7 \to 1$, i.e. $0 \to 1$). If $N = \sum_{i=0}^{6} d_i 10^i$, the image N' satisfies $N' \equiv \sum (d_i + 1)10^i = N + 1111111 \pmod 7$.

Since $1111110 = 7 \cdot 158730$, we get $1111111 \equiv 1$, so $N' \equiv N + 1 \pmod 7$.

Applying the map r times sends the codes with remainder 0 bijectively onto those with remainder r. So the seven remainder classes have equal size, and exactly $5040/7 = 720$ codes are divisible by 7.

Check. 1111111 mod 7 another way: $10 \equiv 3$, and $1 + 3 + 2 + 6 + 4 + 5 + 1 = 22 \equiv 1 \pmod 7$ (powers $3^0, \ldots, 3^6$). Example: $1234567 = 7 \cdot 176366 + 5$ and its image $2345671 = 7 \cdot 335095 + 6$, one higher, as predicted.

5. Answer: 8500**. The idea.** The condition rearranges to $(x-1)(y-1) \equiv 0 \pmod{1000}$. Shifting by 1 is a bijection, so count pairs of residues (u, v) with $uv \equiv 0 \pmod{1000}$, split into mod 8 and mod 125 by the Chinese Remainder Theorem, and count by the power of the prime in u.

Work it out. $xy - x - y + 1 = (x - 1)(y - 1)$, and $u = x - 1$, $v = y - 1$ run over all residues mod 1000 as x, y do. By CRT, $uv \equiv 0 \pmod{1000}$ iff $uv \equiv 0 \pmod 8$ and $uv \equiv 0 \pmod{125}$, and the pair (u, v) mod 1000 corresponds to independent pairs mod 8 and mod 125. So the count is (pairs mod 8) $\times$ (pairs mod 125).

Mod p^k: sort u by $j = v_p(u)$. For $j < k$ there are $\varphi(p^{k-j}) = p^{k-j-1}(p-1)$ such residues, and $uv \equiv 0$ iff $p^{k-j} \mid v$, which leaves p^j choices of v: each j contributes $p^{k-1}(p-1)$. For $u = 0$ every one of the p^k values of v works. Total $kp^{k-1}(p-1) + p^k = p^{k-1}(k(p-1) + p)$.

Mod 8: $4(3 + 2) = 20$. Mod 125: $25(12 + 5) = 425$. Answer $20 \cdot 425 = 8500$.

Check. Mod 8 directly: $u = 0$ gives 8; $u = 4$ needs v even, 4; $u = 2, 6$ need $4 \mid v$, $2 \cdot 2 = 4$; the four odd u need $v = 0, 4$. Total $8 + 4 + 4 + 4 = 20$.

6. Answer: 179**. The idea.** $q = r$ means $n = q(k + 1)$ with $1 \le q < k$. So the valid k correspond to divisors $d = k + 1$ of n that are large compared with n/d. The divisor $d = n$ always works (for $n \ge 3$), so the question is whether a second, smaller divisor works, and the best candidate is the largest proper divisor.

Work it out. If $r = q$ then $n = qk + q = q(k+1)$, and $q = r < k$ with $q \geq 1$ (as $n > 0$). Conversely if $d = k + 1 \geq 3$ divides n and $q = n/d$ satisfies $1 \leq q \leq d - 2$, then $n = qk + q$ is a legal division with remainder q. So valid k correspond to divisors $d \geq 3$ of n with $n/d \leq d - 2$, i.e. $n \leq d(d-2)$. The condition gets easier as d grows.

$d = n$ works iff $n \geq 3$ ($n \leq n(n-2)$). $n = 1, 2$ have no valid k.

For $n \geq 3$, exactly one k means no proper divisor works; the largest proper divisor is n/p with p the least prime factor, so we need $n > (n/p)(n/p - 2)$, i.e. $p > n/p - 2$, i.e. $n < p(p+2)$.

If $n = p$ is prime this holds: the odd primes up to 1000, $168 - 1 = 167$ of them. If n is composite, $n = pm$ with $m \geq p$ having no prime factor below p, and $m < p + 2$. So $m = p$ (giving $n = p^2$) or $m = p + 1$, which has a factor $2 < p$ unless $p = 2$, $m = 3$ ($n = 6$). Prime squares up to 1000: $p \leq 31$, 11 of them. Total $167 + 11 + 1 = 179$.

Check. $n = 6$: $k = 5$ gives $6 = 1 \cdot 5 + 1$; $k = 2$ gives $q = 3, r = 0$; nothing else. $n = 8$ ($8 \geq 2 \cdot 4$): $k = 7$ and $k = 3$ ($8 = 2 \cdot 3 + 2$), two values, correctly excluded. $n = 9$: only $k = 8$ ($k = 2$ gives $q = 4, r = 1$).

7. Answer: 460**. The idea.** The reachable numbers are exactly $s + 47k$ with $s = 2^a 3^b$ and $k \geq 0$. Modulo the prime 47 both 2 and 3 are squares, so only the 23 nonzero square classes can ever be hit; inside each such class everything from the smallest number of the form $2^a 3^b$ upward is reachable. So we find, for each square class, its smallest $2^a 3^b$.

Work it out. *The reachable set.* Every $2^a 3^b + 47k$ is reachable: build $2^a 3^b$ by doubling and tripling, then add 47 k times. Conversely the set of such numbers contains 1 and is closed under the three moves ($2(s + 47k) = 2s + 47 \cdot 2k$, and similarly for $3x$ and $x + 47$). So n is reachable iff $n \geq s$ and $n \equiv s \pmod{47}$ for some $s = 2^a 3^b$.

Which classes. $2 \equiv 49 = 7^2$ and $3 \equiv 144 = 12^2 \pmod{47}$, so every $2^a 3^b$ is a nonzero square modulo 47. There are exactly 23 nonzero squares mod 47 (the squares of $1, \ldots, 23$ are distinct, as $x^2 \equiv y^2$ forces $x \equiv \pm y$). No multiple of 47 and no non-square class is ever reached.

Class minima. List $2^a 3^b$ in increasing order with residues mod 47, keeping only those in a new class: $1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36$ (their own residues), then $48 \equiv 1$ (old), $54 \equiv 7$, $64 \equiv 17$, $72 \equiv 25$, $81 \equiv 34$, $96 \equiv 2$ (old), $108 \equiv 14$, $128 \equiv 34$, $144 \equiv 3$ (old), $162 \equiv 21$, $192 \equiv 4$ (old), $216 \equiv 28$, then $243, 256, 288$ are old $(8, 21, 6)$, $324 \equiv 42$, then $384, 432, 486, 512, 576$ are old $(8, 9, 16, 42, 12)$, and $648 \equiv 37$. That is 23 classes, all of them, so these are the minima m_r.

Count. In class r the reachable $n \leq 1000$ are $m_r, m_r + 47, \ldots$, which number $\lfloor (1000 - m_r)/47 \rfloor + 1$. Since $1000 = 47 \cdot 21 + 13$, the minima $1, 2, 3, 4, 6, 8, 9, 12$ give 22 each (176); $16, 18, 24, 27, 32, 36, 54$ give 21 each (147); $64, 72, 81$ give 20 each (60); 108 gives 19, 162 gives 18, 216 gives 17, 324 gives 15 and 648 gives 8. Total $176 + 147 + 60 + 19 + 18 + 17 + 15 + 8 = 460$.

Check. 5 is not a square mod 47 (the squares below 10 are $1, 2, 3, 4, 6, 7, 8, 9$ as residues: 5 is missing), so $5, 52, 99, \ldots$ are never reached, although 5 is small. In class 37: $37 + 47 \cdot 13 = 648$ is the first reachable member, and indeed $648 = 2^3 \cdot 3^4$. The count also matches a direct search over all numbers reachable without exceeding 1000 (every move increases the number).

8. Answer: 814**. The idea.** By the Chinese Remainder Theorem, n is complete iff every prime power exactly dividing it is. Modulo a prime power, $x^2 + 2y^2$ either factors (when -2 is a square) and hits everything, or it can only be $\equiv 0 \pmod{p}$ when $p \mid x$ and $p \mid y$, which forces a gap modulo p^2.

Work it out. *Odd primes, first power.* For any c, the sets $\{x^2\}$ and $\{c-2y^2\}$ modulo p each have $(p+1)/2$ elements, so they meet: $x^2 \equiv c-2y^2$ for some x, y. So every odd prime p is complete.

-2 *a square mod* p ($p \equiv 1, 3 \pmod 8$, including $p = 3$). Lift $t^2 \equiv -2$ to $t^2 \equiv -2 \pmod{p^k}$ (Hensel, p odd). Then $x^2+2y^2 \equiv (x-ty)(x+ty)$, and $(x, y) \mapsto (x-ty, x+ty)$ is invertible mod p^k because $2t$ is a unit. Taking the factors 1 and c hits every c: all powers of such p are complete.

-2 *not a square* ($p \equiv 5, 7 \pmod 8$). If $p \nmid y$, then $x^2+2y^2 \equiv 0$ would make $-2 \equiv (x/y)^2$; so $x^2+2y^2 \equiv 0 \pmod p$ forces $p \mid y$, then $p \mid x$, and then $p^2 \mid x^2+2y^2$. Hence the residue p is missed modulo p^2, and p^k is incomplete for $k \geq 2$ (a representation mod p^k would give one mod p^2).

Powers of 2. Mod 2 and mod 4: $x^2 \in \{0, 1\}$, $2y^2 \in \{0, 2\}$ give all of $0, 1, 2, 3$. Mod 8: $x^2 \in \{0, 1, 4\}$, $2y^2 \in \{0, 2\}$, sums $\{0, 1, 2, 3, 4, 6\}$: 5 and 7 are missed, so 2^k with $k \geq 3$ is incomplete.

So n is incomplete iff $8 \mid n$ or $p^2 \mid n$ for some $p \equiv 5, 7 \pmod 8$; with $p^2 \leq 1000$ these are $p = 5, 7, 13, 23, 29, 31$. Inclusion–exclusion over $8, 25, 49, 169, 529, 841, 961$: singles $125+40+20+5+1+1+1 = 193$; pairs with product at most 1000 are only $8 \cdot 25 = 200$ (5 multiples) and $8 \cdot 49 = 392$ (2 multiples). Incomplete: $193 - 7 = 186$. Complete: $1000 - 186 = 814$.

Check. $n = 25$: values $x^2+2y^2 \equiv 0 \pmod 5$ need $5 \mid x, y$, so $5 \pmod{25}$ is never reached. $n = 9$: $-2 \equiv 7 \equiv 4^2 \pmod 9$, and indeed e.g. $3 \equiv 1+2\cdot 1$, $6 \equiv 4+2\cdot 1$, $0 \equiv 0$ all appear; 9 is complete.

9. Answer: 4668**. The idea.** Suppose $m \geq n$. Then m^2+7n lies strictly between m^2 and $(m+4)^2$, so it must be $(m+j)^2$ with $j \in \{1, 2, 3\}$; this makes m a linear function of n. Substituting into $n^2+7m = (n+t)^2$ with $t \geq 1$ gives a linear equation $n \cdot (\text{positive number}) = (\text{positive number})$, and the coefficient of n is positive only for finitely many t. Squeezing between squares twice leaves a short finite check.

Work it out. The conditions are symmetric, so find the pairs with $m \geq n$ and then reflect. Since $0 < 7n \leq 7m < 8m+16$, we get $m^2 < m^2+7n < (m+4)^2$, so $m^2+7n = (m+j)^2$ with $j \in \{1, 2, 3\}$, i.e. $7n = 2jm + j^2$ and $m = \dfrac{7n-j^2}{2j}$.

Now $n^2+7m > n^2$, so $n^2+7m = (n+t)^2$ with $t \geq 1$: $2tn+t^2 = 7m = \dfrac{49n-7j^2}{2j}$. Clearing the denominator, $n(49-4jt) = 2jt^2+7j^2$. The right side is positive, so $4jt < 49$, and n must be a positive integer for which m is also a positive integer with $m \geq n$.

$j = 1$: $n(49-4t) = 2t^2+7$ for $t = 1, \ldots, 12$. The right sides $9, 15, 25, 39, 57, 79, 105, 135, 169, 207, 249, 295$ over the left coefficients $45, 41, 37, 33, 29, 25, 21, 17, 13, 9, 5, 1$ are integers only for $t = 7, 9, 10, 12$: $n = 5, 13, 23, 295$, and $m = (7n-1)/2 = 17, 45, 80, 1032$.

$j = 2$: $n(49-8t) = 4t^2+28$ for $t = 1, \ldots, 6$: $32/41$, $44/33$, $64/25$, $92/17$, $128/9$, $172/1$. Only $t = 6$ works: $n = 172$, $m = (7n-4)/4 = 300$.

$j = 3$: $n(49-12t) = 6t^2+63$ for $t = 1, \ldots, 4$: $69/37$, $87/25$, $117/13 = 9$, $159/1 = 159$. So $n = 9$, $m = (63-9)/6 = 9$ and $n = 159$, $m = (1113-9)/6 = 184$.

All seven pairs have $m \geq n$: $(9, 9)$, $(17, 5)$, $(45, 13)$, $(80, 23)$, $(184, 159)$, $(300, 172)$, $(1032, 295)$. Reflecting gives 13 ordered pairs, with $(9, 9)$ counted once. Their values of $m+n$ are 18 once and $22, 58, 103, 343, 472, 1327$ twice each. The sum is $18 + 2 \cdot 2325 = 4668$.

Check. $(17, 5)$: $289+35 = 324 = 18^2$ and $25+119 = 144 = 12^2$. $(1032, 295)$: $1032^2+2065 = 1067089 = 1033^2$ and $295^2+7224 = 94249 = 307^2$ ($t = 12$). $(184, 159)$: $33856+1113 =$

$34969 = 187^2$ and $25281 + 1288 = 26569 = 163^2$.

10. Answer: 34**. The idea.** By CRT, x mod 10000 is the pair (x mod 16, x mod 625), and T acts on each coordinate by the same rule $x \mapsto 3x + 1$. Understand the cycle structure on each factor, then combine: a cycle of length a on one factor and a cycle of length b on the other produce ab pairs that split into $\gcd(a, b)$ cycles of length $\operatorname{lcm}(a, b)$. The key tricks: mod 625, conjugate away the +1 by shifting by $\frac{1}{2}$; mod 16, where 2 is not invertible, use $y = 2x + 1$ modulo 32.

Work it out. *Mod* 625. Let $h = 2^{-1} \pmod{625}$ and $z = x+h$. Then $T(x)+h = 3x+1+h = 3(x+h)$ because $1+h = 3h$ ($2h = 1$). So T is conjugate to $z \mapsto 3z$. Multiplication by 3 preserves the exact power of 5 dividing z. The layer of z with $5^j \| z$ ($j = 0, 1, 2, 3$) is 5^j times the unit group mod 5^{4-j}, on which 3 acts; since 3 is a primitive root modulo every power of 5 (3 has order 4 mod 5 and $3^4 = 81 \not\equiv 1 \pmod{25}$), each layer is a single cycle, of length $\varphi(5^{4-j})$: 500, 100, 20, 4; plus the fixed point $z = 0$. Cycle lengths mod 625: 1, 4, 20, 100, 500.

Mod 16. Put $y = 2x + 1$, read mod 32; $x \mapsto y$ is a bijection from residues mod 16 onto the 16 odd residues mod 32. Then $2T(x) + 1 = 6x + 3 = 3(2x + 1) = 3y \pmod{32}$. So T is conjugate to $y \mapsto 3y$ on the units mod 32. The order of 3 mod 32 is 8 ($3^2 = 9$, $3^4 = 81 \equiv 17$, $3^8 \equiv 289 \equiv 1$), so the 16 units fall into two cycles of length 8.

Combine. Each mod-16 cycle (length 8) paired with the mod-625 cycles of lengths 1, 4, 20, 100, 500 gives $\gcd(8, \cdot) = 1, 4, 4, 4, 4$ cycles, i.e. 17. Two mod-16 cycles: $2 \cdot 17 = 34$.

Check. Count elements: each mod-16 cycle times all of mod 625 gives $8 \cdot 625 = 5000$ elements in 17 cycles, e.g. the 8×500 block splits into 4 cycles of length $\operatorname{lcm}(8, 500) = 1000$: $4 \cdot 1000 = 4000$, plus $8 + 4 \cdot 8 + 4 \cdot 40 + 4 \cdot 200 = 8 + 32 + 160 + 800 = 1000$. Total 5000, as it should be. Small sanity check: the unique fixed point mod 625 is $x = -h = 312$ ($3 \cdot 312 + 1 = 937 \equiv 312$).