MTH 215 Number Theory

Solutions of the problems appearing in the End-Semester Examination

---

Part I

1. **(a)** Let $r := \lfloor\sqrt{p}\rfloor$. Since p is not a perfect square, we have $r^2 < p < (r+1)^2$. Consider the $(r+1)^2$ integers $u + xv$ for $u, v \in \{0, 1, \ldots, r\}$. By the pigeon hole principle, there exist unequal pairs (u_1, v_1) and (u_2, v_2) such that $u_1 + xv_1 \equiv u_2 + xv_2 \pmod{p}$. Let $a := u_1 - u_2$ and $b := v_2 - v_1$. Then $a \equiv bx \pmod{p}$. By the choice of u_1, u_2, v_1 and v_2 it follows that $-r \leqslant a \leqslant r$ and $-r \leqslant b \leqslant r$ with either $a \neq 0$ or $b \neq 0$. Furthermore, since $x \not\equiv 0 \pmod{p}$, both a and b must be non-zero.

(b) Clearly, 2 cannot be expressed in the form $a^2 + 3b^2$ with $a, b \in \mathbb{Z}$. If $p = 3$, take $a = 0$ and $b = 1$. So assume that p is an odd prime > 3. Then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right)$. By the law of quadratic reciprocity we have $\left(\frac{3}{p}\right) = (-1)^{(3-1)(p-1)/4}\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$, i.e., $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Therefore, -3 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{3}$.

First consider the case that $p \equiv 1 \pmod{3}$. Take x to be a square root of -3 modulo p. By Part (a) there exists $a, b \in \mathbb{Z}$ with $0 < |a| < \sqrt{p}$ and $0 < |b| < \sqrt{p}$ such that $a \equiv bx \pmod{p}$. Squaring gives $a^2 \equiv b^2x^2 \equiv -3b^2 \pmod{p}$, i.e., $a^2 + 3b^2 \equiv 0 \pmod{p}$. From the inequalities satisfied by the values of a and b it follows that $0 < a^2 + 3b^2 < 4p$. If $a^2 + 3b^2 = p$, we are done. If $a^2 + 3b^2 = 2p$, then $a^2 \equiv 2 \pmod{3}$, a contradiction. Finally, if $a^2 + 3b^2 = 3p$, then $3|a$, so that $b^2 + 3(a/3)^2 = p$.

Next consider $p \equiv 2 \pmod{3}$. Let $p = a^2 + 3b^2$ for some $a, b \in \mathbb{Z}$. Clearly, $\gcd(a, p) = \gcd(b, p) = 1$. Then $(ab^{-1})^2 \equiv -3 \pmod{p}$, a contradiction, since -3 is a quadratic nonresidue modulo p.

2. **(a)** If g is a quadratic residue modulo p, by Euler's criterion we have $g^{(p-1)/2} \equiv 1 \pmod{p}$. But then $\operatorname{ord}_p g < p - 1$ and hence g cannot be a primitive root modulo p.

(b) Let g be a primitive root modulo p. Then $g^0, g^2, g^4, \ldots, g^{p-3}$ are distinct modulo p and are quadratic residues modulo p. Since there are $(p-1)/2$ quadratic residues modulo p, it follows that these are all the quadratic residues modulo p. The quadratic nonresidues modulo p are then $g, g^3, g^5, \ldots, g^{p-2}$.

[If] Let $p = 2^{2^n} + 1$ and let a be a quadratic nonresidue modulo p. Then $a \equiv g^{2k+1} \pmod{p}$ for some k and $\operatorname{ord}_p a = (\operatorname{ord}_p g)/\gcd(\operatorname{ord}_p g, 2k+1) = 2^{2^n}/\gcd(2^{2^n}, 2k+1) = 2^{2^n} = p - 1$. Thus a is a primitive root modulo p.

[Only if] Since p is odd we can write $p = 2^t u + 1$, where $t, u \in \mathbb{N}$ and u is odd. g^u is a quadratic nonresidue modulo p and has order $p - 1 = 2^t u$ by hypothesis. But $\operatorname{ord}_p g^u = 2^t u/\gcd(2^t u, u) = 2^t$. Therefore, we must have $u = 1$, i.e., $p = 2^t + 1$. Now we write $t = 2^n s$ for $n \in \mathbb{Z}_+$, $s \in \mathbb{N}$ and s odd. But then $2^{2^n} + 1$ divides p. Since p is a prime, this forces $s = 1$.

3. If $m \in \mathbb{N}$ is not square-free, then $\mu(m) = 0$. Hence the given sum equals $\sum_{m \in \mathcal{F}'(n)} \mu(m)$, where $\mathcal{F}'(n) := \{m \in \mathcal{F}(n) \mid m \text{ is square-free}\}$. If $p_1, \ldots, p_r \in \mathbb{P} \setminus \{2\}$ are pairwise distinct, then $\phi(p_1 \cdots p_r) = (p_1 - 1)\cdots(p_r - 1) = (2-1)(p_1 - 1)\cdots(p_r - 1) = \phi(2p_1 \cdots p_r)$, whereas $\mu(p_1 \cdots p_r) + \mu(2p_1 \cdots p_r) = (-1)^r + (-1)^{r+1} = 0$. Therefore, in the given sum we can pair $\mu(m)$ for each odd $m \in \mathcal{F}'(n)$ with $\mu(2m)$, since we also have $2m \in \mathcal{F}'(n)$. Hence the result follows.

4. Let $\langle a_0, a_1, a_2, \ldots\rangle$ be the infinite simple continued fraction expansion of $\sqrt{2}$. One can easily check that $a_0 = 1$ and $a_1 = a_2 = a_3 = \cdots = 2$. For each $n \in \mathbb{Z}_+$ let $h_n/k_n = \langle a_0, \ldots, a_n\rangle$ be the nth convergent to $\sqrt{2}$. Then for every $n \in \mathbb{Z}_+$ we have $\left|\sqrt{2} - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}} = \frac{1}{k_n(2k_n + k_{n-1})} \leqslant \frac{1}{2k_n^2}$, i.e., $\sqrt{2}k_n - \frac{1}{2k_n} < h_n < \sqrt{2}k_n + \frac{1}{2k_n}$, i.e., $-\sqrt{2} + \frac{1}{4k_n^2} < h_n^2 - 2k_n^2 < \sqrt{2} + \frac{1}{4k_n^2}$. Since $k_n \geqslant 1$, it follows that $h_n^2 - 2k_n^2 \in \{0, 1, -1\}$ for all $n \in \mathbb{Z}_+$. But $\sqrt{2}$ is irrational, so we cannot have $h_n^2 - 2k_n^2 = 0$. Also note that $\frac{h_n}{k_n} < \sqrt{2}$ for even n, whereas $\frac{h_n}{k_n} > \sqrt{2}$ for odd n. It, therefore, follows that $h_n^2 - 2k_n^2 = \begin{cases} -1 & \text{if } n \text{ is even,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$

Part II

5. $22021 = 19^2 \times 61$ is not prime.

6. The given triple can be rewritten as $(F_{n+2}^2 - F_{n+1}^2, 2F_{n+1}F_{n+2}, F_{n+2}^2 + F_{n+1}^2)$ from which the first statement follows. The triple may not be primitive, since F_{n+2} and F_{n+1} may be of the same parity, in which case 2 divides both the first and second components of the given triple. However, if F_{n+2} and F_{n+1} are of opposite parities, then the triple is primitive, since $\gcd(F_{n+2}, F_{n+1}) = 1$.

7. [If] Let $m = M_{p_1} \cdots M_{p_r}$, where M_{p_i} are distinct Mersenne primes. Since σ is multiplicative, it follows that $\sigma(m) = (1 + M_{p_1}) \cdots (1 + M_{p_r}) = 2^{p_1} \cdots 2^{p_r} = 2^{p_1 + \cdots + p_r}$.

[Only if] Let $m = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ be the canonical prime factorization of m. Then $\sigma(m) = \sigma(q_1^{\alpha_1}) \cdots \sigma(q_r^{\alpha_r})$. In particular, each $\sigma(q_i^{\alpha_i}) = 1 + q_i + q_i^2 + \cdots + q_i^{\alpha_i}$ is a power of two and hence even. It follows that both q_i and α_i are odd, in which case $1 + q_i$ divides $\sigma(q_i^{\alpha_i})$ and hence is again a power of 2. Thus $q_i = 2^{p_i} - 1 = M_{p_i}$ for some $p_i \in \mathbb{N}$. Since q_i is prime, p_i has to be prime, so that $q_i = M_{p_i}$ is a Mersenne prime. We finally show that $\alpha_i = 1$. Assume otherwise, i.e., $\alpha_i > 1$. We have seen that $\alpha_i = 2k + 1$ is odd. We then have $\sigma(q_i^{\alpha_i}) = (1+q_i)(1+q_i^2+q_i^4+\cdots+q_i^{2k})$. Thus $1+q_i^2+q_i^4+\cdots+q_i^{2k}$ is a power of 2 and, in particular, even, so that k is odd, say $2l+1$ and, therefore, $1+q_i^2+q_i^4+\cdots+q_i^{2k} = (1+q_i^2)(1+q_i^4+q_i^8+\cdots+q_i^{4l})$. This implies that $1+q_i^2$ is a power of 2, a contradiction, since $1+q_i^2 = 1+M_{p_i}^2 = 1+(2^{p_i}-1)^2 = 2(1+2^{p_i}(2^{p_i-1}-1))$ has an odd divisor greater than 1.

8. If $a = b$, then $(a^2 + b^2)/(1 + ab) = 2a^2/(1 + a^2)$ is an integer if and only if $a = 1$, in which case $(a^2 + b^2)/(1 + ab) = 1$, a perfect square. So assume that $(a^2 + b^2)/(1 + ab) = m \in \mathbb{N}$ for some $a, b \in \mathbb{N}$, $a > b$. We now recursively construct a sequence $x_1, x_2, x_3, \ldots$ of integers such that $(x_i^2 + x_{i+1}^2)/(1 + x_i x_{i+1}) = m$ for each i and $x_1 > x_2 > x_3 > \cdots$. We start by setting $x_1 := a$ and $x_2 := b$. Assume that $x_1, \ldots, x_i$ are constructed for some $i \geqslant 2$ and each of $x_1, \ldots, x_i$ is positive. Since $(x_{i-1}^2 + x_i^2)/(1 + x_{i-1}x_i) = m$ we have $x_{i-1}^2 - (mx_i)x_{i-1} + (x_i^2 - m) = 0$. The polynomial $f(x) := x^2 - (mx_i)x + (x_i^2 - m) \in \mathbb{Z}[x]$ has two complex roots of which one is x_{i-1}. Let the other root be x_{i+1}. Then $x_{i+1} = mx_i - x_{i-1} \in \mathbb{Z}$. The quantity $x_i(x_i - x_{i-1})$ is negative and hence less than m, so that $x_i > (x_i^2 - m)/x_{i-1} = x_{i+1}$, since the product of the two roots of f is $x_i^2 - m$. Finally, $f(x_{i+1}) = 0$ implying that $(x_i^2 + x_{i+1}^2)/(1 + x_i x_{i+1}) = m$.

Since x_i form a strictly decreasing sequence of integers, it follows that for some $r \geqslant 2$ the integer x_{r+1} is negative, whereas $x_r \geqslant 0$. If $x_r > 0$, then $1 + x_r x_{r+1}$ is either 0 or negative and hence $(x_r^2 + x_{r+1}^2)/(1 + x_r x_{r+1})$, if defined at all, cannot equal m which is positive. So we must have $x_r = 0$ and hence $(x_{r-1}^2 + x_r^2)/(1 + x_{r-1}x_r) = m$ implies that $m = x_{r-1}^2$.

(**Remark:** But then, do there exist such funny pairs (a, b)? The answer is "yes". For every $n \in \mathbb{N}$ taking $a = n^3$ and $b = n$ gives $(a^2 + b^2)/(1 + ab) = n^2$. There are other solutions too. My computer says that all the triples (a, b, m) with $0 < b \leqslant a \leqslant 1000$ are $(1, 1, 1)$, $(8, 2, 4)$, $(27, 3, 9)$, $(30, 8, 4)$, $(64, 4, 16)$, $(112, 30, 4)$, $(125, 5, 25)$, $(216, 6, 36)$, $(240, 27, 9)$, $(343, 7, 49)$, $(418, 112, 4)$, $(512, 8, 64)$, $(729, 9, 81)$ and $(1000, 10, 100)$. Do you see an interesting pattern, i.e., in all these cases $\gcd(a, b) = \sqrt{m}$? This easily follows from the facts that $\gcd(x_{r-1}, x_r) = \sqrt{m}$ and that $x_{i-1} = mx_i - x_{i+1}$.)

9. Unless otherwise stated, in this exercise we denote by $\{x\}$ the fractional part of a real number x, i.e., $\{x\} := x - \lfloor x \rfloor$. We start with the following lemma which states the interesting result that the fractional parts of the integral multiples of an irrational number constitute a dense subset of the closed interval $[0, 1]$. I provide two elementary proofs of the lemma. The first is based on the theory of continued fractions and the second on a cute elementary trick.

Lemma: Let ξ be an irrational number and let $0 < a < b < 1$. There exist infinitely many $n \in \mathbb{N}$ with the property that $a < \{n\xi\} < b$.

First proof We may assume without loss of generality that a and b are rationals (because we may replace a and b by rationals a' and b' satisfying $a \leqslant a' < b' \leqslant b$). Since $a < b$, we can choose a positive real number

D (perhaps an integer) large enough such that $\lceil aD \rceil \leqslant \lfloor bD \rfloor$. Clearly for every real $\Delta \geqslant D$ we continue to have $\lceil a\Delta \rceil \leqslant \lfloor b\Delta \rfloor$. Since ξ is irrational, there exists $c/d \in \mathbb{Q}$ such that $d \geqslant D$ and $0 < d\xi - c < 1/d$. Call $\Delta := 1/(d\xi - c)$. Then $\Delta > d \geqslant D$ and, therefore, $\lceil a\Delta \rceil \leqslant \lfloor b\Delta \rfloor$. Choose any integer m satisfying $\lceil a\Delta \rceil \leqslant m \leqslant \lfloor b\Delta \rfloor$ and consider the irrational $\zeta := m(d\xi - c)$. Then $\zeta \geqslant \lceil a\Delta \rceil (d\xi - c) > a\Delta(d\xi - c) = a$, where the last inequality is strict, since $a\Delta = a/(d\xi - c)$ is irrational (under the assumption that a is rational). Similarly, $\zeta \leqslant \lfloor b\Delta \rfloor (d\xi - c) < b\Delta(d\xi - c) = b$. Thus $a < \{\zeta\} < b$. But $\{\zeta\} = \{md\xi\}$. Therefore, there exists an $n \in \mathbb{N}$ such that $a < \{n\xi\} < b$.

To prove that there are infinitely many such n assume otherwise. Let $n_1, \ldots, n_k$ be all the positive integers with this property. Choose β such that $a < \beta < \min(\{n_1\xi\}, \ldots, \{n_k\xi\}) < b$. The above argument establishes the existence of an $n \in \mathbb{N}$ such that $a < \{n\xi\} < \beta$. But then $a < \{n\xi\} < b$, whereas $n \neq n_i$ for all $i = 1, \ldots, k$, a contradiction. •

Second proof As in the first proof we start by showing that there exists an $n \in \mathbb{N}$ with the stated property. Assume otherwise, i.e., the interval (a, b) does not contain any of $\{\xi\}, \{2\xi\}, \{3\xi\}, \ldots$. Since ξ is irrational and hence $\{n\xi\} \neq 0, 1$ for all $n \in \mathbb{N}$, we may join the end points 0 and 1 and visualize the interval $[0, 1]$ as a circle of circumference 1. Let A_0 be a *maximal* open arc on this circle that contains the interval (a, b) and no points of the form $\{n\xi\}$. For each $m \in \mathbb{N}$ let A_m denote the open arc generated by elements $\{\alpha - m\xi\}$ for all $\alpha \in A_0$. If A_m contains a point $\{n\xi\}$, then A_0 would contain $\{(n + m)\xi\}$, a contradiction. Thus each A_m also contains no points of the form $\{n\xi\}$. Now each A_m has the same length as A_0. If $A_m = A_{m'}$ for $m \neq m'$, then we would have $\{\alpha - m\xi\} = \{\alpha - m'\xi\}$ for every $\alpha \in A_0$. This cannot hold, since this implies that ξ is rational. So the intervals $A_0, A_1, \ldots$ are pairwise distinct. They are also pairwise disjoint, since a non-empty intersection of A_m with $A_{m'}$ $(m > m')$ implies a non-empty intersection of $A_{m-m'}$ with A_0 violating the maximality of A_0. Thus our circle of unit circumference contains an infinite number of pairwise disjoint open arcs each of length $\geqslant b - a > 0$. This is absurd.

To prove the infinitude of the natural numbers n with $a < \{n\xi\} < b$ assume that there are only finitely many such values of n, say $n_1, \ldots, n_k$. Take any $\nu \in \mathbb{N}$ with $\nu > \max(n_1, \ldots, n_k)$. Repeating the above argument on $\{\nu\xi\}, \{(\nu + 1)\xi\}, \{(\nu + 2)\xi\}, \ldots$ produces an $n \geqslant \nu$ such that $a < \{n\xi\} < b$, a contradiction, since $n > n_i$ for all $i = 1, \ldots, k$. •

Let us now come to the problem. Take $\xi := \log_{10} 2$, $a := \log_{10} 2.002$ and $b := \log_{10} 2.003$. Let $n \in \mathbb{N}$ be any one of the infinite integers satisfying $a < \{n\xi\} < b$, i.e., $l + \log_{10} 2.002 < n \log_{10} 2 < l + \log_{10} 2.003$ for some integer $l \in \mathbb{N}$, $l \geqslant 3$. Raising to the power of 10 then gives $2002 \times 10^{l-3} < 2^n < 2003 \times 10^{l-3}$.

(**Remark:** A small GP-PARI program reveals the secret that the smallest such n is 1652 and we have

$$
\begin{aligned}
2^{1652} = {} & 2002409222782325408497265157147301050387645361578432632413268642985190 47 \backslash \\
& 0862319335622152734966680937610412985288510424547917182350071120554168 04 \backslash \\
& 1694065756051007646232612881305886777965002285280446988135836909497721 95 \backslash \\
& 5865301104536661811067263929883919333386245985511789400064287058856663 91 \backslash \\
& 8174485772377350790229768620938715953179722904883379128105856727385202 26 \backslash \\
& 4267011529089886014269314934200028066746211548312967292117014241928057 04 \backslash \\
& 157770375663448827029891741801092565772509222301608766470405226496\,.
\end{aligned}
$$

The program also told me that all the values of n less than one million having this property are 1652, 3788, 14953, 17089, 19225, 28254, 30390, 32526, 41555, 43691, 45827, 56992, 59128, 61264, 70293, 72429, 74565, 85730, 87866, 90002, 99031, 101167, 103303, 112332, 114468, 116604, 127769, 129905, 132041, 141070, 143206, 145342, 156507, 158643, 160779, 169808, 171944, 174080, 183109, 185245, 187381, 198546, 200682, 202818, 211847, 213983, 216119, 227284, 229420, 231556, 240585, 242721, 244857, 253886, 256022, 258158, 269323, 271459, 273595, 282624, 284760, 286896, 295925, 298061, 300197, 302333, 311362, 313498, 315634, 324663, 326799, 328935, 340100, 342236, 344372, 353401, 355537, 357673, 366702, 368838, 370974, 382139, 384275, 386411, 395440, 397576, 399712, 410877, 413013, 415149, 424178, 426314, 428450, 437479, 439615, 441751, 452916, 455052, 457188, 466217, 468353, 470489, 481654, 483790, 485926, 494955, 497091, 499227, 508256, 510392, 512528, 523693, 525829, 527965, 536994, 539130, 541266, 552431, 554567, 556703, 565732, 567868, 570004, 579033, 581169, 583305, 594470, 596606, 598742, 607771, 609907, 612043, 621072, 623208, 625344, 627480, 636509, 638645, 640781, 649810, 651946, 654082, 665247, 667383, 669519, 678548, 680684, 682820, 691849, 693985, 696121, 707286, 709422, 711558, 720587, 722723, 724859, 736024, 738160, 740296, 749325, 751461, 753597, 762626, 764762, 766898, 778063, 780199, 782335, 791364, 793500, 795636, 806801, 808937, 811073, 820102, 822238, 824374, 833403, 835539, 837675, 848840, 850976, 853112, 862141, 864277, 866413, 877578, 879714, 881850, 890879, 893015, 895151, 904180, 906316, 908452, 919617, 921753, 923889, 932918, 935054, 937190, 946219, 948355, 950491, 952627, 961656, 963792, 965928, 974957, 977093, 979229, 990394, 992530 and 994666. There are 215 of them! There are 2 of them less than 10^4 and 21 less than 10^5. Again there seems to be a pattern: $2, 21, 215$. But this is too small an evidence to jump to a conclusion. Both our proofs of the lemma provide existential certificates for an infinite number of n with $a < \{n\xi\} < b$. Counting the number of all such n less than a given bound seems to be a much more difficult task.

The first proof of the above lemma can be modified a bit to conclude that given any $t \in \mathbb{N}$ there exist t relevant values of n that are in arithmetic progression. The above list reveals an example for $t = 5$, namely, 527965, 583305, 638645, 693985 and 749325. There may be longer sequences in the list.)

10. Let the set $S := \{z \in \mathbb{N} \mid x^4 - x^2y^2 + y^4 = z^2 \text{ for some } x, y \in \mathbb{N}, x \neq y\} \subseteq \mathbb{N}$ be non-empty. Then S has a smallest element. Call it Z and let $X^4 - X^2Y^2 + Y^4 = Z^2$ with $X, Y \in \mathbb{N}$, $X \neq Y$. Because of symmetry we may assume without loss of generality that $X > Y$. Let $g := \gcd(X, Y)$. Then the triple $(X/g, Y/g, Z/g^2)$ satisfies the given Diophantine equation and hence $Z/g^2 \in S$. By minimality of Z we then must have $g = 1$.

We have $(X^2 - Y^2)^2 + (XY)^2 = Z^2$, i.e., $(X^2 - Y^2, XY, Z)$ is a Pythagorean triple. The condition $\gcd(X, Y) = 1$ implies that this triple is primitive. Since X and Y cannot be both even, we consider the following two cases.

Case 1: X and Y are both odd.

By the characterization of primitive Pythagorean triples we have:

$$XY = r^2 - s^2, \quad X^2 - Y^2 = 2rs \quad \text{and} \quad Z = r^2 + s^2$$

for some coprime $r, s \in \mathbb{N}$, $r > s$, r and s having opposite parities. Easy calculations show that the triple $(r, s, (X^2+Y^2)/2)$ satisfies the given Diophantine equation, so that $(X^2+Y^2)/2 \in S$. But $XY < Z$ (since $(X^2 - Y^2)^2 + (XY)^2 = Z^2$) and $(X^2 + Y^2)^2 = (X^2 - Y^2)^2 + X^2Y^2 + 3X^2Y^2 = Z^2 + 3X^2Y^2 < 4Z^2$, i.e., $(X^2 + Y^2)/2 < Z$. This contradicts the minimality of Z in S.

Case 2: X and Y are of opposite parities.

We consider the case X is even and Y is odd. The proof for the other case would be similar. Once again by the characterization of primitive Pythagorean triples we have:

$$X^2 - Y^2 = r^2 - s^2, \quad XY = 2rs \quad \text{and} \quad Z = r^2 + s^2$$

for some coprime $r, s \in \mathbb{N}$, $r > s$, r and s having opposite parities. We assume that r is even and s is odd. The other case can be treated similarly. We start with the following prime factorizations of X, Y, r and s, that comply with the equations $XY = 2rs$ and $\gcd(X, Y) = \gcd(r, s) = 1$:

$$\begin{aligned}
X &= 2^{\gamma} p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}, \\
Y &= p_{k+1}^{\alpha_{k+1}} \cdots p_{k+u}^{\alpha_{k+u}} q_{l+1}^{\beta_{l+1}} \cdots q_{l+v}^{\beta_{l+v}}, \\
r &= 2^{\gamma-1} p_1^{\alpha_1} \cdots p_{k+u}^{\alpha_{k+u}} \text{ and} \\
s &= q_1^{\beta_1} \cdots q_{l+v}^{\beta_{l+v}},
\end{aligned}$$

where p_i and q_j are pairwise distinct odd primes. We further define the following gcds:

$$\begin{aligned}
P_1 &= \gcd(X, r) &&= 2^{\gamma-1} p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \\
P_2 &= \gcd(X, s) &&= q_1^{\beta_1} \cdots q_l^{\beta_l}, \\
Q_1 &= \gcd(Y, r) &&= p_{k+1}^{\alpha_{k+1}} \cdots p_{k+u}^{\alpha_{k+u}} \text{ and} \\
Q_2 &= \gcd(Y, s) &&= q_{l+1}^{\beta_{l+1}} \cdots q_{l+v}^{\beta_{l+v}}.
\end{aligned}$$

We then have $X = 2P_1P_2$, $Y = Q_1Q_2$, $r = P_1Q_1$, $s = P_2Q_2$. Plugging in these values in $X^2 - Y^2 = r^2 - s^2$ gives $P_1^2(4P_2^2 - Q_1^2) = Q_2^2(Q_1^2 - P_2^2)$. But $\gcd(P_1, Q_2) = 1$. Therefore there is an integer ρ such that

$$Q_1^2 - P_2^2 = \rho P_1^2 \quad \text{and} \quad 4P_2^2 - Q_1^2 = \rho Q_2^2.$$

From these equations we get

$$3P_2^2 = \rho(P_1^2 + Q_2^2) \quad \text{and} \quad 3Q_1^2 = \rho(4P_1^2 + Q_2^2).$$

We thus have $3 = \gcd(3P_2^2, 3Q_1^2) = \rho \gcd(P_1^2 + Q_2^2, 4P_1^2 + Q_2^2) = \rho \gcd(P_1^2 + Q_2^2, 3P_1^2)$. Now P_1 and Q_2 cannot be both divisible by 3 (since they are coprime). Hence considering all possible values of P_1 and Q_2 modulo 3, we see that $P_1^2 + Q_2^2$ is congruent to 1 or 2 modulo 3. This forces $\rho = 3$ and hence it follows that

$$P_2^2 = P_1^2 + Q_2^2 \quad \text{and} \quad Q_1^2 = 4P_1^2 + Q_2^2.$$

$(Q_2, 2P_1, Q_1)$ is, therefore, a primitive Pythagorean triple and we have integers $c > d > 0$, $\gcd(c, d) = 1$ such that

$$Q_2 = c^2 - d^2, \quad 2P_1 = 2cd \quad \text{and} \quad Q_1 = c^2 + d^2.$$

But then $P_2^2 = P_1^2 + Q_2^2$ implies that $(c^2 - d^2)^2 + c^2d^2 = P_2^2$. Hence (c, d, P_2) is a solution of the given Diophantine equation and $P_2 \in S$. But $Z = r^2 + s^2 > s^2 = P_2^2Q_2^2 \geqslant P_2$. This once again contradicts the minimality of Z in S.
