2018 Stellenbosch Mathematics Camp
Senior Number Theory Problem Set

Robin Visser

December 2018

1 Diophantine equations

1. Solve for positive integers m, n:
$$1 + 5 \cdot 2^m = n^2$$

Solution: We have $(n-1)(n+1) = 5 \cdot 2^m$. Note that n is odd, which implies both $n-1$ and $n+1$ are even. Furthermore, $\gcd(n-1, n+1) = 2$. Therefore, we have either $v_2(n-1) = 1$ or $v_2(n+1) = 1$. Noting the cases for 5, this yields the following possibilities:

$$\begin{aligned} & n-1 = 2 \quad \text{or} \quad n-1 = 10 \\ \text{or} \quad & n+1 = 2 \quad \text{or} \quad n+1 = 10 \end{aligned}$$

Noting all cases, one obtains that only $n = 9$ yields a valid solution where $m = 4$. Thus the only solution is $(n, m) = (9, 4)$. $\square$

2. Solve for $m, n \in \mathbb{Z}$:
$$9m^2 + 3n = n^2 + 8$$

Solution: We consider the equation as a quadratic in n

$$n^2 - 3n + 8 - 9m^2 = 0$$

Solving for the discriminant Δ yields

$$\Delta = 9 - 4(8 - 9m^2) = 36m^2 - 23$$

For n to be an integer, we require Δ to be a perfect square. Thus $36m^2 - 23 = l^2$ for some $l \geq 0$. Factoring, we obtain $(6m + l)(6m - l) = 23$. As 23 is prime, this yields

$$6m \mp l = \pm 1 \quad \text{and} \quad 6m \pm l = \pm 23$$

Solving this system yields $m - 2$ and $l = 11$, or $m = -2$ and $l = 11$. This therefore gives the following four solutions: $(m, n) \in \{(2, -4), (2, 7), (-2, -4), (-2, 7)\}$. $\square$

3. Solve for $a, d \in \mathbb{Z}$:
$$a^4 + 120a = d^2$$

Solution: Note if $a = 0$, then $d = 0$. Assuming now that $a > 0$, we have $a^4 < d^2$. Thus $(a^2 + 1)^2 \leq d^2 = a^4 + 120a$. This yields the following inequality for a:

$$2a^2 - 120a + 1 \leq 0$$

This implies $0 < a < 60$. A very tedious way to conclude, is to check all remaining cases. An alternate approach is to bound d^2 by a weaker interval, such as noting that $a^4 < d^2 < (a^2+6)^2$ for $a \geq 10$. Then we only need to check the cases $0 < a < 10$, otherwise assuming $a \geq 10$, we have either $d = a^2+2$ or $d = a^2+4$, noting that the parity of a and d are the same.

Doing this approach, we note that $a \in \{1,2,3,5\}$ yields valid solutions for $0 < a < 10$. Otherwise, substituting $d = a^2+2$ or $d = a^2+4$ into the given equation yields no further solutions.

Doing the same approach for negative integers a, we obtain

$$(a,d) \in \{(0,0),(1,\pm 11),(2,\pm 16),(3,\pm 21),(5,\pm 35),(-5,\pm 5),(-6,\pm 24),(8,\pm 56)\}.$$

$\square$

Remark: The factor 120 can be made smaller to reduce case checking. One can also restrict to strictly positive integer solutions.

4. Solve for $x, y \in \mathbb{Z}$:

$$7^x + x^4 + 47 = y^2$$

Solution: First consider the equation mod 4. This yields $(-1)^x + x^4 - 1 \equiv y^2 \pmod 4$. Assuming that x is odd, this furthermore gives $x^4 - 2 \equiv y^2 \pmod 4$. However, as squares (and thus fourth powers) are only 0 or 1 (mod 4), this gives a contradiction.

Therefore x is even. Let $x = 2a$. This gives $7^{2a} + 16a^4 + 47 = y^2$. Note that $(7^a)^2 < y^2$, thus $(7^a+1)^2 \leq y^2$, which yields

$$\begin{aligned} 7^{2a} + 2 \cdot 7^a + 1 \leq y^2 &= 7^{2a} + 16a^4 + 47 \\ \implies 7^a &\leq 8a^4 + 23 \end{aligned}$$

Now, one can easily prove by induction that this is false if $a \leq 4$. Thus $a \in \{1,2,3\}$. Checking each case yields the only solution is $a = 2$, thus we have $(x,y) = (4,52)$ as the only solution. $\square$

5. Determine all pairs (a,b) of integers with the property that the numbers a^2+4b and b^2+4a are both perfect squares.

Solution: If either a or b is 0, then both must be perfect squares. If $a = b$, then we must solve $a^2 + 4a = k^2$ where $k \in \mathbb{Z}$. This gives us $(a+2-k)(a+2+k) = 4$ which can easily be solved to give the solution $a = b = -4$. If $a = -b$, then we similarly obtain $(a-2-k)(a-2+k) = 4$ which yields no solutions.

We can now assume $|a| > |b| \geq 1$. If $|a| > 4$, we have

$$(|a|-4)^2 = a^2 - 8|a| + 16 \leq a^2 - 4|a| \leq a^2 + 4b \leq a^2 + 4|a| < (|a|+2)^2$$

This bounds a^2+4b between two squares. Furthermore, noting that a^2+4b and b^2+4a have the same pairty, we thus have that either $a^2+4b = a^2$ or $a^2+4b = (|a|-2)^2$. The former case yields $b = 0$ which has been covered, thus we assume $a^2+4b = (|a|-2)^2$, which implies $b = 1 - |a|$.

Therefore, $b^2 + 4a = a^2 - 2|a| + 1 + 4a$ is a perfect square. We consider two cases:

Case 1: $a > 0$. Thus $b^2 + 4a = a^2 + 2a + 1 = (a+1)^2$ which is a square.

Case 2: $a < 0$. Thus $b^2 + 4a = a^2 + 6a + 1 = (a+3)^2 - 8$. Now, the only case which will give two squares a difference of 8 apart is $1, 9$, which yields $a = -6$ and $b = -5$.

Finally, we consider the cases where $|a| \leq 4$. This only yields the solution $(-4, -4)$. We thus conclude the solutions are

$$\begin{aligned} & a = 0 \text{ and } b = k^2, \quad k \geq 0 \\ \text{or} \quad & a = k^2 \text{ and } b = 0, \quad k \geq 0 \\ \text{or} \quad & a = k \text{ and } b = 1 - k, \quad k \in \mathbb{Z} \\ \text{or} \quad & (a, b) \in \{(-4,-4), (-5,-6), (-6,-5)\} \end{aligned}$$

□

6. Find all positive integers a, b such that $a! + b! = a^b + b^a$.

   Solution: We first consider $a = b$. Thus $a! = a^a$ which only has the solution $a = 1$. We now assume wlog that $a > b$. We consider two cases:

   Case 1: $\gcd(a, b) > 1$. Let p be prime such that $p \mid \gcd(a, b)$ and let $a = pm$ and $b = pn$. Thus

   $$(pm)! + (pn)! = (pm)^{pn} + (pn)^{pm}$$

   Noting the highest power of p dividing the equation, we have

   $$v_p(LHS) = v_p((pm)!+(pn)!) = v_p((pn)!) = \sum_{k=1}^{\infty} \left\lfloor \frac{pn}{p^k} \right\rfloor < \sum_{k=1}^{\infty} \frac{pn}{p^k} = \frac{pn}{p-1} \leq pn \leq v_p(RHS)$$

   which gives a contradiction.

   Case 2: $\gcd(a, b) = 1$. We define $k = b - a$, where $k > 0$ and $\gcd(b, k) = 1$. Therefore

   $$(b+k)! + b! = (b+k)^b + b^{b+k}$$

   Now clearly $b \mid ((b+k)! + b!)$, thus $b \mid (b+k)^b$. By the binomial theorem, this implies $b \mid k^b$. However, noting that b, k are coprime, this yields $b = 1$. Thus $a! + 1 = a + 1$, which implies $a = 2$ (as $a > b = 1$).

   Therefore we have the solutions $(a, b) \in \{(1,1), (1,2), (2,1)\}$. □

7. Solve for $x, y, z \in \mathbb{Z}$:

   $$2(x^2 + y^2 + z^2) = (x-y)^3 + (y-z)^3 + (z-x)^3$$

   Solution: Consider the left hand side $(x-y)^3 + (y-z)^3 + (z-x)^3$. Note that this evaluates to 0 if $x = y$ or $y = z$ or $z = x$. Thus $(x-y)$, $(y-z)$ and $(z-x)$ are all factors. (one can check this explicitly as well). Quotienting out these factors from the LHS yields a quotient of 3. We thus obtain

   $$2(x^2 + y^2 + z^2) = 3(x-y)(y-z)(z-x)$$

   Todo conclude. Solutions, up to cyclic order and sign are

   $$\{(0,0,0), (10,20,25), (30,40,70), (65,70,125), (91,104,143), \\ (105,150,165), (115,130,175), (140,259,266) \ldots\}$$

   .

2 Divisibility

1. Prove that n does not divide $2^n - 1$ for all positive integers $n > 1$.

   Solution: Assume for contradiction that $n > 1$ such that n divides $2^n - 1$. Clearly $2^n - 1$ is always odd, thus n must be odd. Let p be the smallest prime dividing n. Thus p divides $2^n - 1$. Therefore

   $$2^n \equiv 1 (\text{mod } p)$$

   However, by Fermat's Little, we have

   $$2^{p-1} \equiv 1 (\text{mod } p)$$

   Thus, the order of 2 (mod p) must divide both n and $p-1$. However, as p is the smallest odd prime diving n, we have n and $p-1$ are coprime (noting n is odd). Thus the order of 2 (mod p) is 1, which is a contradiction. $\square$

   Remark: Perhaps this can be generalised to determine the n which is coprime to $2^n - 1$.

2. Prove that n does not divide $2^{n-1} + 1$ for all positive integers $n > 1$.

   Solution: Doing a contradiction argument, let p be a prime divisor of n. Thus $2^{n-1} \equiv -1$ (mod p) which implies $2^{2(n-1)} \equiv 1$ (mod p). Let t denote the order of 2 modulo p. Thus $t \mid 2(n-1)$ and $t \not| (n-1)$. Let $n - 1 = 2^k u$ where u is odd. We thus have $2^{k+1} \mid t$. Now, by Fermat's Little, $t \mid p - 1$. We thus have $2^{k+1} \mid p - 1$, which implies $p \equiv 1$ (mod 2^{k+1}) for all prime divisors p of n. Thus $n \equiv 1$ (mod 2^{k+1}), and thus $2^{k+1} \mid n - 1$, which clearly contradicts u being odd. $\square$

3. Let p be an odd prime. Prove that $(p-1)^p + 1$ is divisible by p^2, but not divisible by p^3.

   Solution: We use the binomial theorem. Note

   $$\begin{aligned}
   (p-1)^p + 1 &= \sum_{k=0}^{\infty} \binom{p}{k} p^k (-1)^{p-k} + 1 \\
   &= \sum_{k=2}^{\infty} \binom{p}{k} p^k (-1)^{p-k} + \binom{p}{1} p^1 (-1)^{p-1} + + \binom{p}{0} p^0 (-1)^{p-0} + 1 \\
   &= \sum_{k=2}^{\infty} \binom{p}{k} p^k (-1)^{p-k} + p^2
   \end{aligned}$$

   noting that p is odd, thus $(-1)^p = -1$. We also note that $\binom{p}{k} p^k$ is divisible by p^3 for all $k \geq 2$. Thus

   $$(p-1)^p + 1 = \sum_{k=2}^{\infty} \binom{p}{k} p^k (-1)^{p-k} + p^2 \equiv p^2 \pmod{p^3}$$

   which proves the claim. $\square$

4. Prove that for each prime number p and positive integer n, p^n divides

   $$\binom{p^n}{p} - p^{n-1}$$

   Solution: The case $p = 2$ can easily be verified. Now, assume p is an odd prime. Note

   $$\binom{p^n}{p} - p^{n-1} = \frac{(p^n)!}{p!(p^n - p)!} - p^{n-1} = p^{n-1} \frac{(p^n - 1)!}{(p-1)!(p^n - p)!} - p^{n-1} = p^{n-1} \left(\binom{p^n - 1}{p - 1} - 1 \right)$$

Thus p^n divides $\binom{p^n}{p} - p^{n-1}$ iff p divides $\binom{p^n-1}{p-1} - 1$. Noting that $(p-1)!$ is coprime to p, we have

$$\begin{aligned} & \binom{p^n-1}{p-1} \equiv 1 \pmod{p} \\ \iff \quad & (p^n-1)(p^n-2)\dots(p^n-p+1) \equiv 1\cdot 2 \dots (p-1) \pmod{p} \end{aligned}$$

Reducing modulo p, we obtain $(-1)^{p-1}(p-1)! \equiv (p-1)!$ (mod p) which is clearly true as p is odd. □

5. If positive integers a, b, c are such that b divides a^3, c divides b^3, and a divides c^3, prove that abc divides $(a+b+c)^{13}$.

   Solution: We easily note that a, b, c must all have the same prime factors. Let p be a prime which divides a (and thus b and c). We note

$$\begin{aligned} v_p((a+b+c)^{13}) = 13v_p(a+b+c) &\geq 13\min\{v_p(a), v_p(b), v_p(c)\} \\ &= (3^2+3+1)\min\{v_p(a), v_p(b), v_p(c)\} \\ &\geq v_p(a)+v_p(b)+v_p(c) = v_p(abc) \end{aligned}$$

   Noting this for each prime factor p, we obtain that abc divides $(a+b+c)^{13}$. □

   Remark: Indeed, one can prove more generally that if b divides a^n, c divides b^n and a divides c^n, then abc divides $(a+b+c)^{n^2+n+1}$.

3 Sequences

1. Suppose $a_1, a_2, \dots$ is an infinite strictly increasing sequence of positive integers and $p_1, p_2, \dots$ is a sequence of distinct primes such that $p_n \mid a_n$ for all $n \geq 1$ and such that $a_n - a_k = p_n - p_k$ for all $n, k \geq 1$. Prove that the sequence (a_n) consists only of prime numbers.

   Solution: Let $c = a_1 - p_1$, and assume for contradiction that $c \geq 1$. For all n, we have $a_n - p_n = a_1 - p_1 = c$. Now, as $p_n \mid a_n$, we have $p_n \mid (a_n - p_n) = c$, thus $p_n \leq c$. Hence $a_n = c + p_n \leq 2c$. This implies the sequence (a_n) is bounded which is a contradiction. Thus $c = 0$, which implies $a_n = p_n$ for all n. □

2. Show that there exists an infinite arithmetic progression of natural numbers such that the first term is 16 and the number of positive divisors of each term is divisible by 5. Of all such sequences, find the one with the smallest possible positive common difference.

   Solution: Note that the sequence given by $a_k = 16 + 32k$ satisfies the problem condition, as $16 + 32k = 2^4(2k+1)$, thus $v_2(a_k) = 4$, which proves $4 + 1 = 5$ divides the number of divisors for all k.

   Secondly, we note that the smallest possible common difference is 32, as the next smallest number after 16 that has number of divisors a multiple of 5 is $48 = 2^4 \cdot 3$. (indeed, if $n = p_1^{a_1} \dots p_k^{a_k}$, then $d(n) = (a_1+1)\dots(a_k+1)$, which implies $5 \mid (a_i+1)$ for some i. Thus, $a_i \geq 4$ for some i). □

3. Let k be a positive integer and let $a_1, a_2, a_3, \dots$ be a sequence of positive integers which satisfies

$$\sum_{d \mid n} a_d = k^n$$

for all $n \geq 1$. Prove that n divides a_n for all $n \geq 1$.

Solution: Given a positive integer k, we note that the sequence a_i is uniquely defined.

Here's a combinatorial solution: Consider an alphabet with k letters. Note that the number of strings of length n is k^n. Now, define $f(d)$ as the number of strings of length d with period d (i.e. it cannot be expressed as a repeated string of smaller length, such as "`abcabc`"). By construction, every string of length n can be paired up with the string representing its period (i.e. "`abcabc`" maps to "`abc`"). We therefore have

$$\sum_{d|n} f(d) = k^n$$

By uniqueness of a_n, this implies $a_n = f(n)$. Also, by construction of $f(n)$, we note that the strings of length n, period n can be partitioned into sets of size n by cycling each string through its n distinct cyclic representations (i.e. "`abc`" yields { "`abc`", "`bca`", "`cab`" }. Thus, we clearly note by construction that n divides $f(n)$ and thus n divides a_n. □

Remark: One can also use Mobius inversion to obtain

$$a_n = \sum_{d|n} \mu(d) k^d$$

Another approach is to use induction.

4. Let $a_0 = a_1 = 1$ and $a_{n+1} = 7a_n - a_{n-1} - 2$ for all positive integers n. Prove that a_n is a perfect square for all n.

Solution:

Let $a_0 = a_1 = 1$ and $a_{n+1} = 7a_n - a_{n-1} - 2$ for all positive integers n. Prove that a_n is a perfect square for all n.

Checking the first few cases, we find $a_2 = 2^2$, $a_3 = 5^2$, $a_4 = 13^2$, squares of every other term of the Fibonacci sequence defined by the equalities $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 2$. This suggests that $a_n = F_{2n-1}^2$ for all $n \geq 1$, which we will prove by induction.

The claim is true for $n = 1, 2, 3, 4$. Assuming $a_k = F_{2k-1}^2$ for $k \leq n$, and subtracting $a_n = 7a_{n-1} - a_{n-2} - 2$ from $a_{n+1} = 7a_n - a_{n-1} - 2$, we obtain

$$\begin{aligned} a_{n+1} &= 8a_n - 8a_{n-1} + a_{n-2} \\ &= 8F_{2n-1}^2 - 8F_{2n-3}^2 + F_{2n-5}^2. \end{aligned}$$

It is not difficult to check that $F_{m-2} = 3F_m - F_{m+2}$ for all $m \geq 2$. Thus, replacing F_{2n-5} by $3F_{2n-3} - F_{2n-1}$ yields

$$\begin{aligned} a_{n+1} &= 8F_{2n-1}^2 - 8F_{2n-3}^2 + (3F_{2n-3} - F_{2n-1})^2 \\ &= (3F_{2n-1} - F_{2n-3})^2 = F_{2n+1}^2, \end{aligned}$$

completing the proof. ■

A similar argument proves the more general result:

If k is an integer greater than 1, $a_0 = a_1 = 1$ and

$$a_{n+1} = (k^2 - 2)a_n - a_{n-1} - 2(k-2) \quad \textit{for } n \geq 1,$$

then a_n is a perfect square for all n. More precisely, $a_n = b_n^2$, where b_n is the general term of the sequence given by $b_0 = b_1 = 1$ and $b_{n+1} = kb_n - b_{n-1}$ for $n \geq 1$.

5. Let $p_1 = 2$ and define a sequence of prime numbers $p_1, p_2, p_3, \ldots$ such that, for all positive integers n, p_{n+1} is the least prime factor of $n \cdot p_1^{1!} \cdot p_2^{2!} \ldots p_n^{n!} + 1$. Prove that all primes appear in the sequence.

   Solution: Assume for contradiction the problem claim does not hold, and let p be the smallest (odd) prime not appearing in the sequence. We thus have that p is not the least prime factor of $1 + n \prod_{i=1}^{n} p_i^{i!}$ for all i. Let C be the smallest integer such that all primes less than p appear in $p_1, p_2, \ldots, p_C$. Thus, if p divides $1 + n \prod_{i=1}^{n} p_i^{i!}$ for some $i > C$, then it must be the smallest factor.

   Therefore, p does not divide $1 + n \prod_{i=1}^{n} p_i^{i!}$ for all $i > C$. Now, define $T_m = \prod_{i=1}^{m} p_i^{i!}$. By Fermat's Little, we have for sufficiently high i and p_i, $p_i^{i!} \equiv 1 \pmod{p}$. Thus, the residue class of T_m stays constant for sufficiently high m. Therfore, there exists an m high enough such that $mT_m \equiv -1 \pmod{p}$, which proves that p divides $1 + mT_m$, which is a contradiction. $\square$

4 Miscellaneous

1. Let
$$E(x, y) = \frac{x}{y} + \frac{x+1}{y+1} + \frac{x+2}{y+2}.$$

   (a) Find all integers $x, y \in \mathbb{Z}$ such that $E(x, y) = 3$.

   (b) Prove that there are infinitely many natural numbers n such that$E(x, y) = n$ has at least one solution in $x, y \in \mathbb{Z}$

   Solution:

   (a) If $x < y$, then clearly $E(x, y) < 3$. Likewise, if $x > y$, then clearly $E(x, y) > 3$. Thus $x = y$, which easily checks to be a solution.

   (b) For any $k \in \mathbb{Z}$, let $n = 11k + 3$. Then $x = 6k + 1$ and $y = 1$ yields a solution to $E(x, y) = n$.

   $\square$

2. Prove that $m + n \leq \gcd(m, n) + \operatorname{lcm}(m, n)$ for all positive integers m, n. When does equality occur?

   Solution: Let $d = \gcd(m, n)$, and denote $m = da$ and $n = db$. We note that $\operatorname{lcm}(m, n) = mn/d$. Thus, dividing the given inequality by d gives a sufficient inequality to prove is $a + b \leq 1 + ab$ for all positive itnegers a, b. However, this is simply $(a-1)(b-1) \leq 0$ which is clearly true for all $a, b \geq 1$. Equality occurs only if either $a = 1$ or $b = 1$, which occurs iff m or n equals d, which occurs iff m divdes n or n divides m. $\square$

3. Let $a < b$ be natural numbers such that for all prime numbers $p > b$, at least one of a and b divides $p - 1$. Prove that $a \leq 2$.

   Solution: Consider the arithmetic sequence $a_n = abn - 1$. By Dirichlet's theorem, this sequence contains infinitely many prime numbers (noting that clearly $\gcd(ab, 1) = 1$). Let $abk - 1$ be some prime number in this sequence. By the problem condition, either a or b divides $abk - 2$. However, as a and b both divide abk, this implies either a or b divides 2. Since $a < b$, this yields $a \leq 2$. $\square$

4. Let $a = 222\ldots 2$ where the digit 2 is denoted 2018 times. Prove that there are no positive integers x, y such that $a = xy(x+y)$.

   Solution: Assume for contradiction such an $x, y \in \mathbb{Z}$ exists. We consider a modulo 9: $a \equiv 2 \cdot 2018 = 4036 \equiv 4 \pmod 9$. Thus 3 does not divide a, and therefore 3 does not divide either x, y, or $x+y$. Thus, we may let $x = 3m \pm 1$ and $y = 3n \pm 1$ where the $\pm$ sign is the same for both x and y. Note

$$\begin{aligned} xy(x+y) &= (3m \pm 1)(3n \pm 1)(3m + 3n \pm 2) \\ &= (9mn \pm 3(m+n) + 1)(3(m+n) \pm 2) \\ &\equiv (\pm 3(m+n) + 1)(3(m+n) \pm 2) \\ &= \pm 9(m+n) + 9(m+n) \pm 2 \\ &\equiv \pm 2 \pmod 9 \end{aligned}$$

   As $\pm 2 \not\equiv 4 \pmod 9$, this yields a contradiction. $\square$

   Remark: The question can easily be generalised to any digit d and length l such that $dl \not\equiv \pm 2 \pmod 9$

5. If $f : \mathbb{N} \to \mathbb{R}$ is a function such that

$$\prod_{d|n} f(d) = 2^n$$

   holds for all $n \in \mathbb{N}$, show that f sends $\mathbb{N}$ to $\mathbb{N}$.

   Solution: First, assuming the existence of such a function, we note f is unique. Letting $n = 1$ yields $f(1) = 2$. By induction, assuming the known values $f(1), f(2), \ldots, f(k-1)$, letting $n = k$ yields a unique value for $f(k)$.

   We now simply note that $f(n) = 2^{\phi(n)}$ is a valid solution which sends $\mathbb{N}$ to $\mathbb{N}$, noting the well-known result that $\sum_{d|n} \phi(d) = n$ $\square$

6. Find all positive integers $n \geq 2$ such that $n^{n-1} - 1$ is square-free.

   Solution: First, note that if $n = 2$, then $n^{n-1} - 1 = 1$ which is not square-free. Now, consider n odd. Thus n is either 1 or 3 (mod 4). As $n - 1$ is even, this implies n^{n-1} is 1 (mod 4), and thus 4 divides $n^{n-1} - 1$, hence not square-free.

   Now, assume $n \geq 4$ even, and consider some $p \mid (n-1)$. Note, p is odd and clearly p does not divide either n or 1. Thus, by lifting the exponent lemma, we have

$$v_p(n^{n-1} - 1) = v_p(n^{n-1} - 1^{n-1}) = v_p(n-1) + v_p(n-1) = 2v_p(n-1) \geq 2$$

   Hence p^2 divides $n^{n-1} - 1$ and is thus not square-free. Therefore, only $n = 2$ satisfies the problem condition. $\square$

7. Let m and n be two integers such that both the quadratic equations $x^2 + mx - n = 0$ and $x^2 - mx + n = 0$ have integer roots. Prove that n is divisible by 6.

   Solution: Let a, b be the two (not necessarily distinct) roots of $x^2 + mx - n = 0$ and let c, d be the two (not necessarily distinct) roots of $x^2 - mx + n = 0$. By Vieta, we have $ab = -n$, $a + b = -m$ and $cd = n$, $c + d = m$. Now, adding the four equations

$$\begin{aligned} a^2 + ma - n = 0, &\quad b^2 + mb - n = 0, \\ c^2 - mc + n = 0, &\quad d^2 - md + n = 0, \end{aligned}$$

yields

$$a^2+b^2+c^2+d^2+m(a+b-c-d)=0 \implies a^2+b^2+c^2+d^2=2m^2$$

Assuming for contradiction that n is odd, this implies all of a,b,c,d odd, and thus m is even. Therefore

$$a^2+b^2+c^2+d^2=2m^2\equiv 0 \pmod 8$$

However, $a^2\equiv b^2\equiv c^2\equiv d^2\equiv 1 \pmod 8$, which yields a contradiction. Thus n is even. Now assume for contradiction n is not divisible by 3. Thus, none of a,b,c,d is divisible by 3, which implies $a^2\equiv b^2\equiv c^2\equiv d^2\equiv 1 \pmod 3$. Thus

$$2m^2=a^2+b^2+c^2+d^2\equiv 4 \pmod 3 \implies m^2\equiv 2 \pmod 3$$

which yields a contradiction. Thus, 3 divides n and therefore n is divisible by 6. □

8. Show that for any positive integers a and b, $(36a+b)(a+36b)$ cannot be a power of 2.

   Solution: Assume for contradiction $(36a+b)(a+36b)=2^l$ for some $l\le 0$. Let $d=\gcd(a,b)$ and let $a=dm$ and $b=dn$ with $\gcd(m,n)=1$. Note that $d\mid 2^l$, thus $d=2^k$ for some $k\ge 0$. Diving by d^2 on both sides yields $(36m+n)(36n+m)=2^{l-2k}$. Note that $(36m+n)$ is a power of 2 not less than 36. As $4\mid 36$, we have $4\mid n$. By symmetry, this implies $4\mid m$, which contradicts m,n coprime. □

9. Denote by $a \bmod b$ the remainder of the euclidean division of a by b. Determine all pairs of positive integers (a,p) such that p is prime and

   $$a \bmod p + a \bmod 2p + a \bmod 3p + a \bmod 4p = a+p.$$

   Solution: Taking both sides modulo p, we obtain $3a\equiv 0 \pmod p$, thus either $p=3$ or $p\mid a$. We also note that LHS $\le (p-1)+(2p-1)+3p-1)+(4p-1)$. This bounds $a\le 9p-4$. Thus, if $p=3$, then $a\le 23$. Checking each case yields $a=1$ or $a=17$. Otherwise, as $a\le 9p-4$ and $p|a$, this implies $a\in\{p,2p,3p,4p,5p,6p,7p,8p\}$. Checking each case gives only $a=3p$ as a solution. Thus the solutions are

   $$(a,p)=(1,3) \quad \text{or} \quad (a,p)=(17,3) \quad \text{or} \quad a=3p, p \text{ prime}$$

   □

10. Prove that there exist infinitely many even positive integers k such that for every prime p the number p^2+k is composite.

    Solution: We note that any k which is even, and $k\equiv 2 \pmod 3$ and such that $k+9$ is composite will suffice. Indeed, if $p=2$, then $k+4$ is even and ≥ 2 and thus composite. If $p=3$, then $k+9$ is composite by definition. If $p>3$, then $p^2\equiv 1 \pmod 3$. Thus $k+p^2\equiv 0 \pmod 3$, which implies p^2+k is composite.

    Several standard arguments can be given to show infinitely many such k exist. Indeed, the infinite arithmetic progression $k=66l+2$ works. One can also argue using the fact that there exist arbitrarily long consecutive sequences of composite numbers. □

11. An integer $n>1$ and a prime p are such that n divides $p-1$, and p divides n^3-1. Prove that $4p-3$ is a perfect square.

    Solution: From $p\mid n^3-1$, we obtain $p\mid(n-1)(n^2+n+1)$. If $p\mid(n-1)$, then $p\le n-1$, which contradicits $n\le p-1$. Thus $p\mid(n^2+n+1)$. We let $p-1=nm$. Thus $m\le n+1$, since $nm + 1 \mid (n^2 + n + 1)$.

If $m < n+1$, take $m = n-k$. $p = n(n-k)+1 \implies p|n(k+1) \implies p|k+1 \implies p = nm+1 \leq n-m+1 \implies nm \leq n-m$ But this is a contradiction.

Thus $n = m+1$, which gives $p = n(n+1)+1$ and thus $4p-3 = 4(n^2+n+1)-3) = (2n+1)^2$ which proves $4p-3$ is a perfect square. $\square$

12. Let p be an odd prime. Find all primes p for which the quotient

$$\frac{2^{p-1}-1}{p}$$

is a square.

Solution: As p is odd, let $p = 2k+1$, and assume that the given quotient is a^2. This yields $(2^{2k}-1) = pa^2 \implies (2^k-1)(2^k+1) = pa^2$. Now, either p divides 2^k-1 or p divides 2^k+1. If p divides 2^k-1, then

$$\left(\frac{2^k-1}{p}\right)(2^k+1) = x^2$$

with both factors on the left being integers. We also note that $\gcd(2^k-1, 2^k+1) = 1$, thus $\gcd((2^k-1)/p, 2^k+1) = 1$. Therefore 2^k+1 is a perfect square. Likewise, if p divides 2^k+1, then 2^k-1 is a perfect square.

Case 1: $2^k+1 = m^2$ for some $m \in \mathbb{Z}$. Then $2^k = (m-1)(m+1)$. We conclude $m = 3$, thus $p = 7$.

Case 2: $2^k-1 = m^2$ for some $m \in \mathbb{Z}$. Then $2(2^{k-1}-1) = (m-1)(m+1)$. Note that m is odd, thus $(m-1)(m+1) \equiv 0 \pmod 4$. Assuming $k > 1$, we have $2(2^{k-1}-1) \equiv 2 \pmod 4$ which yields a contradiction. We thus only check $k = 1$, which gives $p = 3$.

Therefore, we have two solutions: $p = 3$ or $p = 7$. $\square$

13. Set $S = \{1, 2, 3, ..., 2018\}$. If among any n pairwise coprime numbers in S there exists at least a prime number, find the minimum of n.

Solution: Let us first consider $n = 15$. Note that the set $\{1, 2^2, 3^2, 5^2, 7^2, \ldots, 43^2\}$ consisting of 1 and the squares of the first 14 primes will work. Thus $n \geq 16$. We now prove that amongst any 16 pairwise coprime elements, at least one is prime.

Let $A = \{a_1, a_2, \ldots, a_n\}$ be a set with $n \geq 16$ pairwise coprime elements, and order it in order of smallest prime dividing each element (if 1 is included, let $a_1 = 1$). Let p_i be the smallest prime dividing a_i. As A pairwise corpime, we have $p_2 < p_3 < p_4 < \ldots p_n$. Thus, as $p_2 \geq 2$, we have $p_n \geq 47$ as 47 is the 15th smallest prime. Now assuming that a_n is not prime, we have $a_n \geq p_n^2 = 2209 > 2018$ which yields a contradiction, thus a_n is prime, which proves $n = 16$ is the minimal satisfying the problem condition. $\square$

Remark: Nothing special about 2018, can easily generalise. For an arbitrary n, just requires a manual computation to check the number of primes $p \leq \sqrt{n}$.

14. Let m and n be given positive integers such that mn divides $m^2 + n^2 + m$. Prove that m is a square of an integer.

Solution: Assume for contradiction m is not square. Thus, there exists a prime factor $p|m$ such that p^{2k+1} divides m and p^{2k+2} does not divide m. Thus, p^{2k+1} divides $m^2 +$

$n^2 + m$, thus it divides n^2, thus p^{k+1} divides n. Therefore p^{2k+2} divides mn, and thus divides $m^2 + n^2 + mn$. However, p^{2k+2} divides m^2 and n^2, and thus p^{2k+2} divides m, contradiction. $\square$

15. Let a, b be two positive integers such that $\gcd(a, b) = 1$. Prove that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

Solution: By Euler-Phi, we have $a^{\phi(b)} \equiv 1 \pmod{b}$ and $b^{\phi(a)} \equiv 1 \pmod{a}$. Noting that $b|b^{\phi(a)}$ and $a|a^{\phi(a)}$, we obtain

$$a|a^{\phi(b)} + b^{\phi(a)} - 1 \quad \text{and} \quad b|a^{\phi(b)} + b^{\phi(a)} - 1$$

As a, b are coprime, this implies $ab|a^{\phi(b)} + b^{\phi(a)} - 1$, which thus proves the problem statement. $\square$

16. Determine all prime numbers p such that p is the sum of all primes less than p.

Solution: The only solution is $p = 5$ (as $5 = 2+3$). Let $S(n)$ denote the sum of all prime numbers less than n. Let p_i denote the i-th prime number. Note that $S(p_3) = S(5) = 5$ and $S(p_4) = S(7) = 10 > 7 = p_4$. Now assume $S(p_i) > p_i$ for some i. Thus $S(p_{i+1}) = p_i + S(p_i) > 2p_i$. However, by Bertrand's postulate $2p_i \geq p_{i+1}$, thus $S(p_{i+1}) > p_{i+1}$. Therefore, by induction $S(p_i) \neq p_i$ for all $i \geq 4$. Thus, the only solution is $p = 5$. $\square$

17. Let p be a prime number. Prove that $2^p + 3^p$ cannot be non-trivial perfect power (i.e. a positive integer of the form a^b where $b > 1$).

Solution: We simply apply lifting the exponent lemma. If $p = 2$, we have $2^2 + 3^2 = 13$ which is not a perfect power. Now assume p is an odd prime. We have

$$v_5(2^p + 3^p) = v_5(2 + 3) + v_5(p) = 1 + v_5(p)$$

Now, if $p \neq 5$, then $v_5(2^p + 3^p) = 1$, which implies $2^p + 3^p$ cannot be perfect power. Otherwise, if $p = 5$, then $2^p + 3^p = 275 = 5^2 \cdot 11$ which is not a perfect power. $\square$

18. Let n be a positive integer and define $S_n = \{1, 2, 3, \ldots, n\}$. We denote a non-empty subset T of S_n as *balanced* if the median of T is equal to the average of T. For each $n \geq 1$, prove that the number of balanced subsets of S_n is odd.

Solution: Define a subset U of S_n as *unbalanced* if it is not balanced. We define a map $f : P(S_n) \to P(S_n)$ given by U maps to $\{n - k + 1 \ : \ k \in U\}$ (i.e. it's a reversal map sending each element k in U to $n - k + 1$). Note we clearly have $f(f(U)) = U$ for all $U \in P(S_n)$. Furthermore, the map flips the relative order of the mean and median of U. Thus, if U is unbalanced, then $f(U) \neq U$.

Therefore, we have paired up each unbalanced set uniquely, proving that there are an *even* number of unbalanced sets. As the total number of non-empty subsets is $2^n - 1$, there are thus an *odd* number of balanced subsets. $\square$

19. Let n be a positive integer and let k be an odd positive integer. Moreover, let a, b and c be integers (not necessarily positive) satisfying the equation

$$a^n + kb = b^n + kc = c^n + ka$$

Prove that $a = b = c$.

Solution: Note that, if any two of a, b, c are equal, then so is the third. Let us now assume for contradiction that a, b, c are all distinct. We thus obtain the equations:

$$k = \frac{b^n - a^n}{b - c} = \frac{c^n - b^n}{c - a} = \frac{a^n - c^n}{a - b}$$

By Pigeonhole principle, at least two of a, b, c must have the same parity. Wlog, assume $a \equiv b \pmod 2$. Then, from $k = (b^n - a^n)/(b - c)$, noting that k is odd, we have $b \equiv c \pmod 2$ and thus require that a and c have the same parity. Thus $a \equiv b \equiv c \pmod 2$.

Now, by the same argument, at least two of a, b, c leave the same remainder mod 4. Wlog, assume $a \equiv b \pmod 4$. Again, from $k = (b^n - a^n)/(b - c)$, we require that $b - c$ divisible by 4, and thus b and c leave the same remainder mod 4 since k must be an odd integer.

We therefore obtain by induction that $a \equiv b \equiv c \pmod{2^k}$ for all $k \geq 1$. Thus, this must imply $a = b = c$. $\square$