Problems in Elementary Number Theory

Volume 1, No. 1, Fall 2008

PEN TEAM: pen@problem-solving.be

Written by members (2007∼)

Andrei Frimu	Moldova
Yimin Ge	Austria
Hojoo Lee	Korea
Peter Vandendriessche	Belgium

and edited by members (2008∼)

Daniel Kohen	Argentina
David Kotik	Canada
Soo-Hong Lee	Korea
Cosmin Pohoata	Romania
Ho Chung Siu	Hong Kong
Ofir Gorodetsky	Israel

Contents

Chapter 1

Problems

Problem 1.0.1 (PEN K12). *(Canada 1969) Let $\mathbb{N} = \{1, 2, 3, \cdots\}$ denote the set of positive integers. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that for all m, $n \in \mathbb{N}$: $f(2) = 2$, $f(mn) = f(m)f(n)$, $f(n + 1) > f(n)$.*

Problem 1.0.2 (PEN H15). *(Balkan Mathematical Olympiad 1998) Prove that there are no integers x and y satisfying $x^2 = y^5 - 4$.*

Problem 1.0.3 (PEN O53). *(Schur Theorem) Suppose the set $M = \{1, 2, \ldots, n\}$ is partitioned into t disjoint subsets $M_1, \ldots, M_t$. Show that if $n \geq \lfloor t! \cdot e \rfloor$ then at least one class M_z contains three elements x_i, x_j, x_k with the property that $x_i - x_j = x_k$.*

Problem 1.0.4 (PEN I11). *(Korea 2000) Let p be a prime number of the form $4k+1$. Show that*

$$\sum_{i=1}^{p-1} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) = \frac{p-1}{2}.$$

Problem 1.0.5 (PEN J11). *(a) Saint-Peterburg, 1998 Let $d(n)$ denote the number of positive divisors of the number n. Prove that the sequence $d(n^2+1)$ does not become strictly monotonic from some point onwards.*

(b) Prove that $d((n^2 + 1)^2)$ does not become monotonic from any given point onwards.

Problem 1.0.6 (PEN A3). *(IMO 1988/6) Let a and b be positive integers such that $ab+1$ divides $a^2 + b^2$. Show that*

$$\frac{a^2 + b^2}{ab + 1} \tag{1.1}$$

is the square of an integer.

Problem 1.0.7 (PEN D2). *(Putnam 1991/B4) Suppose that p is an odd prime. Prove that*

$$\sum_{j=0}^{p} \binom{p}{j} \binom{p+j}{j} \equiv 2^p + 1 \pmod{p^2}.$$

Problem 1.0.8 (PEN O35). *(Romania TST 1998) Let n be a prime and $a_1 < a_2 < \ldots < a_n$ be integers. Prove that $a_1, a_2, \ldots, a_n$ is an arithmetic progression if and only if there exists a partition of $\mathbb{N}_0 = \{0, 1, 2, \ldots, \}$ into n sets $A_1, A_2, \ldots, A_n$ so that*

$$a_1 + A_1 = a_2 + A_2 = \ldots = a_n + A_n, \tag{1.2}$$

where $x + A = \{x + a | a \in A\}$.

Problem 1.0.9 (PEN B6). *Suppose that m does not have a primitive root. Show that*

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m} \tag{1.3}$$

for every a relatively prime to m.

Problem 1.0.10 (PEN O49). *((D. Fomin) [Ams, pp. 12]) Consider the set of all five-digit numbers whose decimal representation is a permutation of the digits $1, 2, 3, 4, 5$. Prove that this set can be divided into two groups, in such a way that the sum of the squares of the numbers in each group is the same.*

Chapter 2

Articles

2.1 Increasing multiplicative functions

1 (Canada 1969) Let $\mathbb{N} = \{1, 2, 3, \cdots\}$ denote the set of positive integers. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that for all $m, n \in \mathbb{N}$: $f(2) = 2$, $f(mn) = f(m)f(n)$, $f(n+1) > f(n)$.

PEN K12

First Solution. To get some idea, we first evaluate $f(n)$ for small positive integers n. It follows from $f(1 \cdot 1) = f(1) \cdot f(1)$ that $f(1) = 1$. By the multiplicity, we get $f(4) = f(2)^2 = 4$. It follows from the inequality $2 = f(2) < f(3) < f(4) = 4$ that $f(3) = 3$. Also, we compute $f(6) = f(2)f(3) = 6$. Since $4 = f(4) < f(5) < f(6) = 6$, we get $f(5) = 5$.

We prove by induction that $f(n) = n$ for all $n \in \mathbb{N}$. We know that it holds for $n = 1, 2, 3$. Now, let $n > 2$ and suppose that $f(k) = k$ for all $k \in \{1, \cdots, n\}$. We show that $f(n+1) = n+1$.

Case 1 $n+1$ is composite. One may write $n+1 = ab$ for some positive integers a and b with $2 \leq a \leq b \leq n$. By the inductive hypothesis, we have $f(a) = a$ and $f(b) = b$. It follows that $f(n+1) = f(a)f(b) = ab = n+1$.

Case 2 $n+1$ is prime. In this case, $n+2$ is even. Write $n+2 = 2k$ for some positive integer k. Since $n \geq 2$, we get $2k = n+2 \geq 4$ or $k \geq 2$. Since $k = \frac{n+2}{2} \leq n$, by the inductive hypothesis, we have $f(k) = k$. It follows that $f(n+2) = f(2k) = f(2)f(k) = 2k = n+2$. From the inequality

$$n = f(n) < f(n+1) < f(n+2) = n+2 \tag{2.1}$$

we see that $f(n+1) = n+1$.

By induction, we conclude that $f(n) = n$ for all positive integers n. □

Second Solution. As in the previous solution, we get $f(1) = 1$. From the multiplicativity of f, we find that $f(2n) = f(2)f(n) = 2f(n)$ for all positive integers n. This implies that

$$f\left(2^k\right) = 2^k \tag{2.2}$$

for all positive integers k. Let $k \in \mathbb{N}$. From the assumption, we obtain the inequality

$$2^k = f\left(2^k\right) < f\left(2^k+1\right) < \cdots < f\left(2^{k+1}-1\right) < f\left(2^{k+1}\right) = 2^{k+1}. \tag{2.3}$$

In other words, the increasing sequence of 2^k+1 positive integers

$$f\left(2^k\right), f\left(2^k+1\right), \cdots, f\left(2^{k+1}-1\right), f\left(2^{k+1}\right) \tag{2.4}$$

lies in the set of 2^k+1 consecutive integers $\{2^k, 2^k+1, \cdots, 2^{k+1}-1, 2^{k+1}\}$. This means that $f(n) = n$ for all $2^k \leq n \leq 2^{k+1}$. Since this holds for all positive integers k, we conclude that $f(n) = n$ for all $n \geq 2$. □

Third Solution. The assumption that $f(mn) = f(m)f(n)$ for all positive integers m and n is too strong. We can establish the following proposition.

Proposition 2.1.1. *(Putnam 1963/A2) Let $f : \mathbb{N} \to \mathbb{N}$ be a strictly increasing function satisfying that $f(2) = 2$ and $f(mn) = f(m)f(n)$ for all relatively prime m and n. Then, f is the identity function on $\mathbb{N}$.*

PROOF Since f is strictly increasing, we find that $f(n+1) \geq f(n)+1$ for all positive integers n. It follows that $f(n+k) \geq f(n)+k$ for all positive integers n and k. We now determine $p = f(3)$. On the one hand, we obtain

$$f(18) \geq f(15)+3 \geq f(3)f(5)+3 \geq f(3)(f(3)+2)+3 = p^2+2p+3. \tag{2.5}$$

On the other hand, we obtain

$$f(18) = f(2)f(9) \leq 2(f(10)-1) = 2f(2)f(5)-2 \leq 4(f(6)-1)-2 = 4f(2)f(3)-6 = 8p-6. \tag{2.6}$$

Combining these two, we deduce $p^2+2p+3 \leq 8p-6$ or $(p-3)^2 \leq 0$. So, we have $f(3) = p = 3$.

We now prove that $f\left(2^l+1\right) = 2^l+1$ for all positive integers l. Since $f(3) = 3$, it clearly holds for $l = 1$. Assuming that $f\left(2^l+1\right) = 2^l+1$ for some positive integer l, we obtain

$$f\left(2^{l+1}+2\right) = f(2)f\left(2^l+1\right) = 2\left(2^l+1\right) = 2^{l+1}+2. \tag{2.7}$$

Since f is strictly increasing, this means that $f\left(2^l+k\right) = 2^l+k$ for all $k \in \{1, \cdots, 2^l+2\}$. In particular, we get $f\left(2^{l+1}+1\right) = 2^{l+1}+1$, as desired.

Now, we find that $f(n) = n$ for all positive integers n. It clearly holds for $n = 1, 2$. Let l be a fixed positive integer. We have $f\left(2^l+1\right) = 2^l+1$ and $f\left(2^{l+1}+1\right) = 2^{l+1}+1$. Since f is strictly increasing, this means that $f\left(2^l+k\right) = 2^l+k$ for all $k \in \{1, \cdots, 2^l+1\}$. Since it holds for all positive integers l, we conclude that $f(n) = n$ for all $n \geq 3$. This completes the proof. □

Fourth Solution. We can establish the following general result.

Proposition 2.1.2. *Let $f : \mathbb{N} \to \mathbb{R}^+$ be a function satisfying the conditions:*

(a) $f(mn) = f(m)f(n)$ for all positive integers m and n, and

(b) $f(n+1) \geq f(n)$ for all positive integers n.

Then, there is a constant $\alpha \in \mathbb{R}$ such that $f(n) = n^\alpha$ for all $n \in \mathbb{N}$.

PROOF We have $f(1) = 1$. Our job is to show that $\frac{\ln f(n)}{\ln n}$ is constant when $n > 1$. Assume to the contrary that

$$\frac{\ln f(m)}{\ln m} > \frac{\ln f(n)}{\ln n} \tag{2.8}$$

for some positive integers $m, n > 1$. Writing $f(m) = m^x$ and $f(n) = n^y$, we have $x > y$ or

$$\frac{\ln n}{\ln m} > \frac{\ln n}{\ln m} \cdot \frac{y}{x} \tag{2.9}$$

So, we can pick a positive rational number $\frac{A}{B}$, where $A, B \in \mathbb{N}$, so that

$$\frac{\ln n}{\ln m} > \frac{A}{B} > \frac{\ln n}{\ln m} \cdot \frac{y}{x}. \tag{2.10}$$

Hence, $m^A < n^B$ and $m^{Ax} > n^{By}$. One the one hand, since f is monotone increasing, the first inequality $m^A < n^B$ means that $f\left(m^A\right) \leq f\left(n^B\right)$. On the other hand, since $f\left(m^A\right) = f(m)^A = m^{Ax}$ and $f\left(n^B\right) = f(n)^B = n^{By}$, the second inequality $m^{Ax} > n^{By}$ means that

$$f\left(m^A\right) = m^{Ax} > n^{By} = f\left(n^B\right) \tag{2.11}$$

This is a contradiction. □

Fifth Solution. It is known that we get the same result when we only assume that f is *monotone* increasing and multiplicative. In fact, in 1946, Paul Erdös proved the following result in [1]:

Theorem 2.1.1. *Let $f : \mathbb{N} \to \mathbb{R}$ be a function satisfying the conditions:*
(a) $f(mn) = f(m) + f(n)$ for all relatively prime m and n, and
(b) $f(n+1) \geq f(n)$ for all positive integers n.
Then, there exists a constant $\alpha \in \mathbb{R}$ such that $f(n) = \alpha \ln n$ for all $n \in \mathbb{N}$.

This implies the following multiplicative result.

Theorem 2.1.2. *Let $f : \mathbb{N} \to \mathbb{R}^+$ be a function satisfying the conditions:*
(a) $f(mn) = f(m)f(n)$ for all relatively prime m and n, and
(b) $f(n+1) \geq f(n)$ for all positive integers n.
Then, there is a constant $\alpha \in \mathbb{R}$ such that $f(n) = n^\alpha$ for all $n \in \mathbb{N}$.

PROOF [1] It is enough to show that the function f is completely multiplicative: $f(mn) = f(m)f(n)$ for all m and n. We split the proof in three steps.

STEP 1 Let $a \geq 2$ be a positive integer and let $\Omega_a = \{x \in \mathbb{N} \mid \gcd(x, a) = 1\}$. Then, we obtain

$$L := \inf_{x \in \Omega_a} \frac{f(x+a)}{f(x)} = 1 \tag{2.12}$$

and

$$f\left(a^{k+1}\right) \leq f\left(a^k\right) f(a) \tag{2.13}$$

for all positive integers k.

[1] We present a slightly modified proof in [2]. For another short proof, see [3].

PROOF OF STEP 1 Since f is monotone increasing, it is clear that $L \geq 1$. Now, we notice that $f(k+a) \geq Lf(k)$ whenever $k \in \Omega_a$. Let m be a positive integer. We take a sufficiently large integer $x_0 > ma$ with $\gcd(x_0, a) = \gcd(x_0, 2) = 1$ to obtain

$$f(2)f(x_0) = f(2x_0) \geq f(x_0 + ma) \geq Lf(x_0 + (m-1)a) \geq \cdots \geq L^m f(x_0) \tag{2.14}$$

or

$$f(2) \geq L^m. \tag{2.15}$$

Since m is arbitrary, this and $L \geq 1$ force to $L = 1$. Whenever $x \in \Omega_a$, we obtain

$$\frac{f\left(a^{k+1}\right) f(x)}{f\left(a^k\right)} = \frac{f\left(a^{k+1}x\right)}{f\left(a^k\right)} \leq \frac{f\left(a^{k+1}x + a^k\right)}{f\left(a^k\right)} = f(ax+1) \leq f\left(ax + a^2\right) = f(a)f(x+a) \tag{2.16}$$

or

$$\frac{f(x+a)}{f(x)} \geq \frac{f\left(a^{k+1}\right)}{f(a)f\left(a^k\right)}. \tag{2.17}$$

It follows that $1 = \inf_{x\in\Omega_a} \frac{f(x+a)}{f(x)} \geq \frac{f\left(a^{k+1}\right)}{f(a)f\left(a^k\right)}$ so that $f\left(a^{k+1}\right) \leq f\left(a^k\right) f(a)$.

STEP 2 Similarly, we have

$$U := \sup_{x\in\Omega_a} \frac{f(x)}{f(x+a)} = 1 \tag{2.18}$$

and

$$f\left(a^{k+1}\right) \geq f\left(a^k\right) f(a) \tag{2.19}$$

for all positive integers k.

PROOF OF STEP 2 The first result immediately follows from Step 1.

$$\sup_{x\in\Omega_a} \frac{f(x)}{f(x+a)} = \frac{1}{\inf_{x\in\Omega_a} \frac{f(x+a)}{f(x)}} = 1. \tag{2.20}$$

Whenever $x \in \Omega_a$ and $x > a$, we have

$$\frac{f\left(a^{k+1}\right) f(x)}{f\left(a^k\right)} = \frac{f\left(a^{k+1}x\right)}{f\left(a^k\right)} \geq \frac{f\left(a^{k+1}x - a^k\right)}{f\left(a^k\right)} = f(ax-1) \geq f\left(ax - a^2\right) = f(a)f(x-a). \tag{2.21}$$

It therefore follows that

$$1 = \sup_{x\in\Omega_a} \frac{f(x)}{f(x+a)} = \sup_{x\in\Omega_a,\, x>a} \frac{f(x-a)}{f(x)} \leq \frac{f\left(a^{k+1}\right)}{f(a)f\left(a^k\right)}. \tag{2.22}$$

STEP 3 From the two previous results, whenever $a \geq 2$, we have $f\left(a^{k+1}\right) = f\left(a^k\right) f(a)$. Then, the straightforward induction gives that

$$f\left(a^k\right) = f(a)^k \tag{2.23}$$

for all positive integers a and k. Since f is multiplicative, whenever

$$n = {p_1}^{k_1} \cdots {p_l}^{k_l} \tag{2.24}$$

gives the standard factorization of n, we obtain

$$f(n) = f\left({p_1}^{k_1}\right) \cdots f\left({p_l}^{k_l}\right) = f\left(p_1\right)^{k_1} \cdots f\left(p_l\right)^{k_l}. \tag{2.25}$$

We therefore conclude that f is completely multiplicative.

□

REFERENCES

1 P. Erdos, *On the distribution function of additive functions*, Ann. of Math., **47**(1946), 1-20

2 E. Howe, *A new proof of Erdös's theorem on monotone multiplicative functions*, Amer. Math. Monthly **93**(1986), 593-595

3 L. Moser and J. Lambek, *On monotone multiplicative functions*, Proc. Amer. Math. Soc., **4**(1953), 544-545

2.2 Three ways to reach a Diophantine equation

2 (Balkan Mathematical Olympiad 1998) Prove that there are no integers x and y satisfying $x^2 = y^5 - 4$.
PEN H15

First Solution. Assume to the contrary that $a^2 = b^5 - 4$ for some integers a and b. First consider when a is even:

Since $b^5 = a^2 + 4$ is even, b is also even. Since $a^2 + 4 = b^5$ is divisible by 2^5, we have $a^2 \equiv -4 \pmod{2^5}$. However, this is a contradiction. This is because even $x^2 \equiv -4 \pmod{16}$ is not possible.

Now, consider the case when a is odd. We rewrite the equation in the form

$$b^5 = a^2 + 4 = (a + 2i)(a - 2i) \tag{2.26}$$

and work on $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$, the ring of Gaussian integers. Since a is odd, we find that $a + 2i$ and $a - 2i$ are relatively prime in $\mathbb{Z}[i]$. (Indeed, if $\alpha \in \mathbb{Z}[i]$ divides both $a + 2i$ and $a - 2i$, then α also divides $(a + 2i) - (a - 2i) = 4i$. In other words, α is a divisor of $4i$. Since α also divides $a + 2i$ and since a is odd, this implies that α is a unit in $\mathbb{Z}[i]$.)

We recall that $\mathbb{Z}[i]$ is a unique factorization domain. Since $a + 2i$ and $a - 2i$ are relatively prime, $b^5 = (a + 2i)(a - 2i)$ guarantees that

$$a + 2i = \lambda_1 {\eta_1}^5, \quad a - 2i = \lambda_2 {\eta_2}^5, \tag{2.27}$$

where $\eta_1, \eta_1 \in \mathbb{Z}[i]$ and λ_1, λ_2 are units in $\mathbb{Z}[i]$. Since $\lambda_1 \in \{1, -1, i, -i\}$, we get $\lambda_1 = {\lambda_1}^5$. Hence, we can write

$$a + 2i = \lambda_1 {\eta_1}^5 = (\lambda_1 \eta_1)^5 . \tag{2.28}$$

After setting $\lambda_1 \eta_1 = p + qi$, where $p, q \in \mathbb{Z}$, it becomes

$$a + 2i = (p + qi)^5. \tag{2.29}$$

Taking conjugates, we also get $a - 2i = (p - qi)^5$. It follows that

$$4i = (a + 2i) - (a - 2i) = (p + qi)^5 - (p - qi)^5 = 2\left(5p^4 q - 10p^2 q^3 + q^5\right) i \tag{2.30}$$

or

$$2 = q\left(5p^4 - 10p^2 q^2 + q^4\right). \tag{2.31}$$

Now, we get back in the game on $\mathbb{Z}$. Since q divides 2, we get $q \in \{-2, -1, 1, 2\}$. Reading the above equation modulo 5, $2 \equiv q^5 \pmod{5}$. Since FERMAT'S LITTLE THEOREM says that $q^5 \equiv q \pmod{5}$, we have $2 \equiv q \pmod{5}$ or $q = 2$. However, plugging $q = 2$ into the above equation, we obtain $2 = 2\left(5p^4 - 40p^2 + 16\right)$ or $3 = p^2(8 - p^2)$. Since p^2 divides 3, we get $p = \pm 1$. However, $p = \pm 1$ means that $p^2(8 - p^2) = 7$. This is a contradiction. □

Second Solution. Now, assume to the contrary that $a^2 = b^5 - 4$ for some integers a and b. As in the first solution, it is easy to show that the case when a is even is impossible. We consider the case when a is odd. So, b is also odd. Since $4 = 6^2 - 2^5$, one may rewrite the equation in the form

$$a^2 + 6^2 = b^5 + 2^5 = (b+2)\left(b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4\right). \tag{2.32}$$

Letting $d_1 = b + 2$ and $d_2 = b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4$, we get

$$a^2 + 6^2 = b^5 + 2^5 = d_1d_2. \tag{2.33}$$

We can exclude the case when $d_1 = -1$ or when $d_2 = -1$. Indeed, $d_1 = -1$ or $b = -3$ implies that

$$a^2 + 6^2 = b^5 + 2^5 = (-3)^5 + 2^5 < 0, \tag{2.34}$$

which is a contradiction. If $d_2 = -1$, then $b^5 + 2^5 = d_1d_2 = -d_1 = -b - 2$ or $b^5 + b = (-2)^5 + (-2)$. Since the function $t \mapsto t^5 + t$ is strictly increasing, we have $b = -2$ or $a^2 = b^5 - 4 = -36 < 0$, which is a contradiction.

We now clam that the integer $b^5 + 2^5 = d_1d_2$ has a prime divisor $q \neq 3$ with $q \equiv -1 \ (mod\ 4)$.

STEP 1 We show that it is not possible that both d_1 and d_2 are divisible by 3. Indeed, if d_1 is divisible by 3, since $b \equiv d_1 - 2 \equiv -2 \ (mod\ 3)$, we find that

$$d_2 \equiv b^4 + (-2)b^3 + (-2)^2b^2 + (-2)^3b + (-2)^4 \equiv 5(-2)^4 \not\equiv 0 \ (mod\ 3). \tag{2.35}$$

STEP 2 If $b \equiv -1 \ (mod\ 4)$, then we get $a^2 \equiv b^5 - 4 \equiv -1 \ (mod\ 4)$, which is impossible. Hence, $b \equiv 1 \ (mod\ 4)$. Since $d_1 \equiv b + 2 \equiv -1 \ (mod\ 4)$ and since $d_1 \neq -1$, we see that $|d_1| > 1$. Since $d_1 \equiv -1 \ (mod\ 4)$ and since $|d_1| > 1$, we see that d_1 has at least one prime divisor congruent to -1 modulo 4.

STEP 3 It follows from $d_1d_2 \equiv b^5 + 2^5 \equiv 1 \ (mod\ 4)$ and from $d_1 \equiv b + 2 \equiv -1 \ (mod\ 4)$ that $d_2 \equiv -1 \ (mod\ 4)$. It follows from this and from $d_2 \neq -1$ that $|d_2| > 1$. Since $d_2 \equiv -1 \ (mod\ 4)$, this implies that d_2 also has at least one prime divisor congruent to -1 modulo 4.

Combining results from STEP 1 through STEP 3, we conclude that at least one of d_1 or d_2 has a prime divisor $q \neq 3$ with $q \equiv -1 \ (mod\ 4)$. Since q divides $b^5 + 2^5 = d_1d_2$, our claim is proved.

Now, we employ the following well-known result.

Proposition 2.2.1. *Let $p \equiv -1 \ (mod\ 4)$ be a prime. Let a and b are integers such that $a^2 + b^2$ is divisible by p . Then, both a and b are divisible by p.*

Since $a^2 + 6^2 = b^5 + 2^5$, this means that q also divides $a^2 + 6^2$. From PROPOSITION 2.2.1, we see that both a and 6 are divisible by q. Since $q \equiv -1 \ (mod\ 4)$ and since q divides 6, we get $q = 3$. This is a contradiction for the choice of q.

Now, we offer two different ways to establish PROPOSITION 2.2.1.

FIRST PROOF Assume to the contrary that at least one of them is not divisible by p. Since p divides a^2+b^2, we see that none of them are divisible by p. Since p divides a^2+b^2, we obtain $a^2 \equiv -b^2 \ (mod\ p)$. Raise both sides of the congruence to the power $\frac{p-1}{2}$ and apply FERMAT'S LITTLE THEOREM to obtain

$$1 \equiv a^{p-1} \equiv (-1)^{\frac{p-1}{2}} b^{p-1} \equiv -b^{p-1} \equiv -1 \ (mod\ p). \tag{2.36}$$

This is a contradiction because p is an odd prime.

SECOND PROOF Again, assume to the contrary that none of them are divisible by p. Since p divides a^2+b^2, we have the congruence $a^2 \equiv -b^2 \ (mod\ p)$ or $\left(ab^{-1}\right)^2 \equiv -1 \ (mod\ p)$. This means that -1 is a quadratic residue modulo p, which is a contradiction for $p \equiv -1 \ (mod\ 4)$. □

Third Solution. Just toss the Diophantine equation $x^2 = y^5 - 4$ on the field $\mathbb{Z}/11\mathbb{Z}$! It turns out that $x^2 - y^5 \equiv -4 \ (mod\ 11)$ has no solutions. Here is an example of straightforward generalizations:

Proposition 2.2.2. *Let $p \equiv -1, 11, -7, 17 \ (mod\ 60)$ be a prime. Then, the equation*

$$y^{\frac{p-1}{2}} = x^2 + 4 \tag{2.37}$$

has no integral solutions.

HINT. Read the equation modulo p! □

2.3 A theorem on sum-free subsets

3 (Schur Theorem) Suppose the set $M = \{1, 2, \ldots, n\}$ is partitioned into t disjoint subsets $M_1, \ldots, M_t$. Show that if $n \geq \lfloor t! \cdot e \rfloor$ then at least one class M_z contains three elements x_i, x_j, x_k with the property that $x_i - x_j = x_k$.

PEN O53

First Solution.

Fact 2.3.1. *Using Taylor Series approximation for the function $f(x) = e^x$ at point 0 for $x = 1$, we obtain the well-known identity*

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots, \tag{2.38}$$

hence

$$t! \cdot e = t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{t!}\right) + \frac{1}{t+1} + \frac{1}{(t+1)(t+2)} + \ldots \tag{2.39}$$

Note that, for $t \geq 2$,

$$\frac{1}{t+1} + \frac{1}{(t+1)(t+2)} + \ldots < \frac{1}{t+1} + \frac{1}{(t+1)^2} + \frac{1}{(t+1)^3} + \ldots = -1 + \frac{1}{1 - \frac{1}{t+1}} = \frac{1}{t}, \tag{2.40}$$

hence $S_t = \lfloor t! \cdot e \rfloor = t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{t!}\right)$. It is easy to see that the sequence $(S_t)_{t \geq 0}$ satisfies the recurrence relation

$$S_t = tS_{t-1} + 1 \tag{2.41}$$

for $t \geq 1$, defining $S_0 = 1$.

Now we can proceed with the solution of the problem. Assume no subset of the partition contains three elements a, b, c so that $a + b = c$. From the recurrence relation we have $t \not| S_t$ hence by Pigeonhole Principle, at least $\left\lfloor \frac{S_t}{t} \right\rfloor + 1 = S_{t-1} + 1$ elements of M are found in the same subset of the partition. Denote this subset by $M_1 = \{x_1, x_2, \ldots, x_k\}$ so that $x_1 < \ldots < x_k$, and $k \geq S_{t-1} + 1$. Consider the set $Y = \{y_1, \ldots, y_{k-1}\}$, defined by $y_i = x_{i+1} - x_1$. Clearly $|Y| = k - 1 \geq S_{t-1}$ and no element of Y is in M_1 (otherwise, if $y_i \in M_1$, then $y_i + x_1 = x_{i+1}$, contradiction). Consequently all elements of Y lie in the remaining $t - 1$ subsets. Using similar arguments, at least $\left\lfloor \frac{k-1}{t-1} \right\rfloor + 1 \geq \left\lfloor \frac{S_{t-1} - 1}{t-1} \right\rfloor + 1 = S_{t-2} + 1$ elements of Y are found in the same subset from the partition of M. Without loss of generality, let M_2 be this subset. Then $M_2 = \{y_1, \ldots, y_s\} = \{x_2 - x_1, \ldots, x_{s+1} - x_1\}$, where $s \geq S_{t-2} + 1$. Because $y_i - y_1 = x_{i+1} - x_2$, we obtain $y_i - y_1 \notin M_1 \cup M_2$. Let $Z = \{y_2 - y_1, \ldots, y_s - y_1\} = \{x_3 - x_2, x_4 - x_2, \ldots, x_{s+1} - x_2\}$. Then the $|Z| \geq S_{t-2}$ elements of Z are in the remaining $t - 2$ subsets of the partition. By an easy induction, we get that the subset $M_i = \{x_i - x_{i-1}, x_{i+1} - x_{i-1}, \ldots, \} = \{y_{i-1} - y_{i-2}, y_i - y_{i-2}, \ldots\}$ of the partition contains at least $S_{t-i} + 1$ elements, using at the induction step the observation that the difference of any two elements of the set M_i, $i > 1$, is the difference of some 2 elements of each of the sets $M_1, \ldots, M_{i-1}$. Moreover for each $j < i$ there is an $z \in M_j$ so that for each $c \in M_i$, there is a $d \in M_j$ so that $c = d - z$.

In the end, the set M_t will contain at least $S_0 + 1 = 2$ elements. Assume $M_t = \{a, b\}$ with

$a < b$. Then the number $b - a$ must be in one of the subsets $M_1, \ldots, M_{t-1}$. Assume $b - a \in M_i$. But b and a, are, again by the construction of the sets (M_j), of the form $z_m - z_k$ and $z_n - z_k$, where $z_m, z_n, z_k \in M_i$. We obtained a contradiction because $(b-a) + z_n = (z_m - z_k) - (z_n - z_k) + z_n = z_m$. □

Second Solution. We use a theorem of Ramsey:

Theorem 2.3.1. *Let $a_1, \ldots, a_k \geq 1$ be positive integers and $k \geq 2$. There exists a smallest positive integer $n = R_k(a_1, \ldots, a_k)$ so that for any coloring with k colors of the complete graph K_n there is an index i, $1 \leq i \leq k$ and a complete subgraph K_{a_i} of K_n with all edges of the same color.*

A proof of this theorem can be found in almost any book on Combinatorics or Graph Theory.

Now we will show that

Proposition 2.3.1. $R_t\left(\underbrace{3, 3, \ldots, 3}_{t \text{ times}}\right) \leq \lfloor t! \cdot e \rfloor + 1$

PROOF We proceed by induction on $t \geq 2$. For $t = 2$ we easily get $R_2(3,3) = 6$. Indeed, $R_2(3,3) > 5$ as a regular pentagon having edges of one color, and diagonals of the other contains no monochromatic triangle. On the other side, every vertex of a K_6 has at least 3 neighbors to which it is joined by edges of the same color, say 1. If any of the edges between these three neighbors has color 1, we are done, otherwise they form a monochromatic triangle with edges of color 2.

Assume the statement true for some $t \geq 2$. Let $n = \lfloor t! \cdot e \rfloor$. We will show it holds for $t + 1$. Let $m = \lfloor (t+1)! \cdot e \rfloor + 1$. Each vertex of K_m is endpoint for $m - 1$ edges. Using the Fact, we have $m - 1 = \lfloor (t+1)! \cdot e \rfloor = 1 + (t+1)\lfloor t! \cdot e \rfloor = 1 + (t+1)n$, so any vertex V of K_m has at least $n + 1$ neighbors with which it is joined by edges of the same color, say color $t+1$. Consider the complete graph G formed by these $n + 1$ vertices. If some vertices A, B of this graph are joined by an edge of color $t+1$, then A, B, V form a monochromatic triangle. Otherwise all edges of G have one of t colors. Since G has $n+1 = \lfloor t! \cdot e \rfloor + 1$ vertices, by the induction hypothesis, it has a monochromatic triangle. Consequently K_m has a monochromatic triangle, so $R_{t+1}\left(\underbrace{3, 3, \ldots, 3}_{t+1 \text{times}}\right) \leq \lfloor (t+1)! \cdot e \rfloor + 1$, and the induction step is over.

The statement of Schur Theorem follows easily from the PROPOSITION 2.3.1. Indeed, let $n = \lfloor t! \cdot e \rfloor$. Now assign to the vertices of a complete graph with $n + 1$ vertices K_{n+1} the numbers $1, 2, \ldots, n, n + 1$. Color each edge (i, j) of K_{n+1} with the color c, where $|i - j| \in M_c$. By Proposition 1 $R_t(3, 3, \ldots, 3) \leq \lfloor t! \cdot e \rfloor + 1 = n + 1$, hence K_{n+1} contains a monochromatic triangle. Let $x < y < z$ be the vertices of this monochromatic triangle. Then $y - x, z - x$ and $z - y$ belong to the same set M_i, for some $1 \leq i \leq t$. Since $(y - x) + (z - y) = (z - x)$ the proof of Schur's Theorem is completed. □

Remark 2.3.1 (Schur Number)**.** *The Schur Number $S(t)$ is defined as the largest positive integer n so that there exists a partition in t subsets of the set $\{1, 2, \ldots, n\}$, no subsets containing three integers x, y, z so that $x + y = z$ (x, y, z need not be different). As of now, only the first 4 exact values of the Schur Number are known, namely $S(1) = 1, S(2) = 4, S(3) = 13$ and $S(4) = 44$. We have proved that $S(t) \leq \lfloor t! \cdot e \rfloor - 1$. This upper bound can be slightly improved to $S(t) \leq \left\lfloor t! \left(e - \frac{1}{24} \right) \right\rfloor - 1$. From among the lower bounds, the following estimations are known: $S(t) \geq 2^t - 1$, $S(t) \geq \frac{3^t - 1}{2}$ and $S(t) \geq c \cdot 321^{\frac{t}{5}}$ for $t > 5$ and some constant c.*

REFERENCES

1 H. L. Abbott and D. Hanson, *A Problem of Schur and Its Generalizations*, Acta Arith., **20**(1972), 175-187.

2 H. L. Abbott and L. Moser, *Sum-free Sets of Integers*, Acta Arith., **11**(1966), 392-396.

3 T. C. Brown, P. Erdo"s, F.R.K. Chung and R. L. Graham, *Quantitative forms of a theorem of Hilbert*, J. Combin. Theory Ser. A, **38**(1985), No. 2, 210-216.

4 F. R. K. Chung, *On the Ramsey Numbers* $N(3, 3, \cdots, 3; 2)$. Discrete Math., **5**(1973), 317-321.

5 F. R. K. Chung and C. M. Grinstead, *A Survey of Bounds for Classical Ramsey Numbers*, J. Graph Theory, **7**(1983), 25-37.

6 A. Engel, *Problem Solving Strategies*, Chapter 4, *The Box Principle.*

7 G. Exoo, A Lower Bound for Schur Numbers and Multicolor Ramsey Numbers of K_3, Electron. J. Combin., **1**(1994), #R8.

8 H. Fredricksen, *Five Sum-Free Sets*, Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1975), 309-314.

9 H. Fredrickson, *Schur Numbers and the Ramsey Numbers* $N(3, 3, ..., 3; 2)$, J. Combin. Theory Ser. A, **27**(1979), 371-379.

10 H. Fredricksen and M. M. Sweet, *Symmetric Sum-Free Partitions and Lower Bounds for Schur Numbers*, Electron. J. Combin., **7**(2000), #R32.

11 G. Giraud, *Une généralisation des nombres et de l'inégalité de Schur*, C.R. Acad. Sc. Paris, Série A, **266**(1968), 437-440.

12 G. Giraud, *Minoration de certains nombres de Ramsey binaires par les nombres de Schur généralises*, C.R. Acad. Sc. Paris, Série A, **266**(1968), 481-483.

13 L. Moser, *An Introduction to the Theory of Numbers*, Chapter 7, *Combinatorial Number Theory*

14 L. Moser; G. W. Walker, Problem E985, Amer. Math. Monthly, **59**(1952), No. 4, 253.

15 J. Nešetřil and M. Rosenfeld, *I. Schur, C.E. Shannon and Ramsey Numbers, a short story*, Discrete Math., **229**(2001), 185-195.

17 A. Robertson, *New Lower Bounds for Some Multicolored Ramsey Numbers*, Electron. J. Combin., **6**(1999), #R12.

18 A. Robertson, *New Lower Bounds Formulas for Multicolored Ramsey Numbers*, Electron. J. Combin., **9**(2002), #R13.

16 S. P. Radziszowski, *Small Ramsey numbers*, Electron. J. Combin., Dynamic Survey 1, July 2002, revision #9.

19 I. Tomescu, *Probleme de Combinatorică şi Teoria Grafurilor*, Chapter 14, *Probleme de tip Ramsey*.

20 J. Fox and D. J. Kleitman, On Rado's Boundedness Conjecture, J. Combin. Theory Ser. A, **113**(2006), 84-100.

21 E. G. Whitehead, *The Ramsey Number* $N(3,3,3,3;2)$, Discrete Math., **4**(1973), 389-396.

22 X. Xiaodong, X. Zheng, G. Exoo and S. Radziszowski, *Constructive Lower Bounds on Classical Multicolor Ramsey Numbers*, Electron. J. Combin., **11**(2004), #R35.

2.4 A hidden symmetry

4 (Korea 2000) Let p be a prime number of the form $4k+1$. Show that

PEN I11

$$\sum_{i=1}^{p-1}\left(\left\lfloor\frac{2i^2}{p}\right\rfloor-2\left\lfloor\frac{i^2}{p}\right\rfloor\right)=\frac{p-1}{2}.$$

First Solution. We begin with an example. We list all quadratic residues of 17:

$$\begin{cases}1^2\equiv 16^2\equiv 1,\ \ 2^2\equiv 15^2\equiv 4,\ \ 3^2\equiv 14^2\equiv 9,\ \ 4^2\equiv 13^2\equiv 16,\\ 5^2\equiv 12^2\equiv 8,\ \ 6^2\equiv 11^2\equiv 2,\ \ 7^2\equiv 10^2\equiv 15,\ \ 8^2\equiv 9^2\equiv 13.\end{cases}\tag{2.42}$$

Hence a list of all quadratic residues of 17 is given by

$$1,\ \ 2,\ \ 4,\ \ 8,\ \ 9,\ \ 13,\ \ 15,\ \ 16.\tag{2.43}$$

Can you see the number theoretical *symmetry*? Yeap! Indeed, in the eyes of modulo 17, it becomes

$$1,\ \ 2,\ \ 4,\ \ 8,\ \ -8,\ \ -4,\ \ -2,\ \ -1.\tag{2.44}$$

In general, the set of quadratic residues of a prime of the form $4k+1$ is symmetric. This observation is the key idea of the solution. We now give two simple lemmas, which proofs we shall omit.

Lemma 2.4.1. *Let a and b integers such that $a\equiv b\ (mod\ p)$. Then,*

$$\left\lfloor\frac{2a}{p}\right\rfloor-2\left\lfloor\frac{a}{p}\right\rfloor=\left\lfloor\frac{2b}{p}\right\rfloor-2\left\lfloor\frac{b}{p}\right\rfloor.\tag{2.45}$$

Lemma 2.4.2. *Let $\alpha\in\mathbb{R}$. Then, we have*

$$\lfloor 2\alpha\rfloor-2\lfloor\alpha\rfloor=\begin{cases}0, & \alpha-\lfloor\alpha\rfloor\in\left[0,\frac{1}{2}\right),\\ 1, & \alpha-\lfloor\alpha\rfloor\in\left[\frac{1}{2},1\right).\end{cases}\tag{2.46}$$

Since p is prime and since $p\equiv 1\ (mod\ 4)$, we see that -1 is a quadratic residue modulo p. It thus follows that an integer k is a quadratic residue modulo p if and only if $-k$ is a quadratic residue modulo p. So we take $\frac{p-1}{4}$ integers $\alpha_1,\cdots,\alpha_{\frac{p-1}{4}}$ in $\{1,\cdots,\frac{p-1}{2}\}$ so that

$$-\alpha_{\frac{p-1}{4}},\cdots,-\alpha_1,\alpha_1,\cdots,\alpha_{\frac{p-1}{4}}\tag{2.47}$$

is the complete list of all quadratic residues modulo p. In other words, this is a permutation of

$$1^2=(p-1)^2,2^2=(p-2)^2,\cdots,\left(\frac{p-1}{2}\right)^2=\left(\frac{p+1}{2}\right)^2\tag{2.48}$$

modulo p. It follows that

$$\begin{cases}\lfloor\frac{2\alpha_i}{p}\rfloor-2\lfloor\frac{\alpha_i}{p}\rfloor=0,\\ \lfloor-\frac{2\alpha_i}{p}\rfloor-2\lfloor-\frac{2\alpha_i}{p}\rfloor=1,\end{cases}\tag{2.49}$$

when $i \in \left\{1, \cdots, \frac{p-1}{4}\right\}$. Therefore

$$\begin{aligned}
& \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{2}} \left(\left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{4}} \left(\left\lfloor \frac{2\alpha_i}{p} \right\rfloor - 2 \left\lfloor \frac{\alpha_i}{p} \right\rfloor \right) + 2 \sum_{i=1}^{\frac{p-1}{4}} \left(\left\lfloor -\frac{2\alpha_i}{p} \right\rfloor - 2 \left\lfloor -\frac{\alpha_i}{p} \right\rfloor \right) \\
= \; & 2 \sum_{i=1}^{\frac{p-1}{4}} 0 + 2 \sum_{i=1}^{\frac{p-1}{4}} 1 \\
= \; & \frac{p-1}{2}.
\end{aligned}$$

□

Second Solution. Since -1 is a quadratic residue modulo p, we can write $\lambda^2 \equiv -1 \; (mod \; p)$ for some $\lambda \in \mathfrak{M}_p := \{1, \cdots, p-1\}$. The number theoretical idea we employ here is the fact that the map $k \mapsto \lambda k$ yields an equivalence relation on the set $\mathfrak{M}_p$. We split the proof in two steps.

Lemma 2.4.3. *Let $\alpha, \beta \notin \mathbb{Z}$ with $\alpha + \beta \in \mathbb{Z}$. Then, we obtain*

$$\lfloor \alpha \rfloor + \lfloor \beta \rfloor = \alpha + \beta - 1. \tag{2.50}$$

In addition to LEMMA 2.4.1 *notice that when $a + b \equiv 0 \; (mod \; p)$ and if p does not divide a and b, we have*

$$\left\lfloor \frac{2a}{p} \right\rfloor - 2 \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2b}{p} \right\rfloor - 2 \left\lfloor \frac{b}{p} \right\rfloor = \left\lfloor \frac{2a}{p} \right\rfloor + \left\lfloor \frac{2b}{p} \right\rfloor - 2 \left(\left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{b}{p} \right\rfloor \right) = 1. \tag{2.51}$$

Lemma 2.4.4. *Let $\zeta : \mathfrak{M}_p \to \mathfrak{M}_p$ be the function with $\zeta(k) \equiv \lambda k \; (mod \; p)$.*

(A) Since the function ζ satisfies the equation $\zeta^{(2)}(k) = \zeta(\zeta(k)) = -k$ for all $k \in \mathfrak{M}_p$, we see that $\zeta^{(4)} = \zeta \circ \zeta \circ \zeta \circ \zeta$ is the identity function on $\mathfrak{M}_p$. The bijection ζ naturally offers a partition of the set $\mathfrak{M}_p$ into sets of the type $\left\{k, \zeta(k), \zeta^{(2)}(k), \zeta^{(3)}(k)\right\} = \{k, \zeta(k), -k, -\zeta(k)\}$.[2]

(B) When $k \in \mathfrak{M}_p$, we obtain

$$\begin{cases} \left\lfloor \frac{2k^2}{p} \right\rfloor - 2 \left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = 1, \\ \left\lfloor \frac{2(-k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{(-k)^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(-k)^2}{p} \right\rfloor - 2 \left\lfloor \frac{\zeta(-k)^2}{p} \right\rfloor = 1. \end{cases} \tag{2.52}$$

Hence each equivalence class $\{k, \zeta(k), -k, -\zeta(k)\}$ which has four distinct elements contributes 2 in the sum.

Since there are $\frac{p-1}{4}$ quadruples, we conclude that the total sum is $\frac{p-1}{2}$.

Proof. The first claim comes easily from the definition of the map ζ. For the second part, since $k^2 + \zeta(k)^2 \equiv 0 \; (mod \; p)$, LEMMA 3 implies the result. □

□

[2] In other words, $\mathfrak{M}_p$ is a union of distinct orbits of ζ.

Third Solution. Since -1 is a quadratic residue modulo p, we can write $\lambda^2 \equiv -1 \ (mod\ p)$ for some $\lambda \in \mathfrak{M}_p := \{1, \cdots, p-1\}$.

Lemma 2.4.5. *Let $\zeta : \mathfrak{M}_p \to \mathfrak{M}_p$ be the function with $\zeta(k) \equiv \lambda k \ (mod\ p)$. Then, the map ζ is a bijection. When $k \in \mathfrak{M}_p$, we obtain*

$$\begin{cases} \left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = \frac{k^2}{p} + \frac{\zeta(k)^2}{p} - 1, \\ \left\lfloor \frac{2k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor = \frac{2k^2}{p} + \frac{2\zeta(k)^2}{p} - 1. \\ \left\lfloor \frac{2k^2}{p} \right\rfloor - 2\left\lfloor \frac{k^2}{p} \right\rfloor + \left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2\left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor = 1. \end{cases}$$

Proof. The first claim comes easily from the definition of the map ζ. Consider the second part. Since p is prime, it is clear that $\frac{k^2}{p} \notin \mathbb{Z}$. Since $k^2 + \zeta(k)^2 \equiv 0 \ (mod\ p)$ or $\frac{k^2}{p} + \frac{\zeta(k)^2}{p} \in \mathbb{Z}$, this and LEMMA 2.4.3 give the first identity. Similarly, LEMMA 2.4.3 yields the second one. The third one follows from these two identities. □

Now, we compute the sum. Set

$$S(p) = \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2k^2}{p} \right\rfloor - 2\left\lfloor \frac{k^2}{p} \right\rfloor \right), \tag{2.53}$$

$$T(p) = \sum_{i=1}^{p-1} \left(\left\lfloor \frac{2\zeta(k)^2}{p} \right\rfloor - 2\left\lfloor \frac{\zeta(k)^2}{p} \right\rfloor \right). \tag{2.54}$$

First, since $\zeta(1), \cdots, \zeta(p-1)$ is a permutation of $1, \cdots, p-1$, we obtain

$$S(p) = T(p).$$

On the other hand, the last summation identity in LEMMA 2.4.5 implies that

$$S(p) + T(p) = p - 1.$$

It therefore follows that $S(p) = T(p) = \frac{S(p)+T(p)}{2} = \frac{p-1}{2}$. □

After seeing these approaches, we invite the reader to think on the following variations:

Proposition 2.4.1. *Let p be a prime number of the form $4k+1$. Show that*

$$(a) \quad \sum_{i=1}^{p-1} \left\lfloor \frac{i^2}{p} \right\rfloor = \frac{(p-1)(p-2)}{3};$$

$$(b) \quad \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{i^2}{p} \right\rfloor = \frac{(p-1)(p-5)}{24};$$

$$(c) \quad \sum_{i=(p+1)/2}^{p-1} \left\lfloor \frac{i^2}{p} \right\rfloor = \frac{(p-1)(7p-11)}{24}.$$

2.5 On the monotonicity of the divisor function

5 PEN J11

(a) *Saint-Peterburg, 1998* Let $d(n)$ denote the number of positive divisors of the number n. Prove that the sequence $d(n^2+1)$ does not become strictly monotonic from some point onwards.

(b) Prove that $d((n^2+1)^2)$ does not become monotonic from any given point onwards.

Solution for (a). Intuitively, the sequence being required to be strictly monotonic points that it will eventually grow rather *fast*. This is a hint to the solution. Note that if n is even, then the set of divisors of n^2+1 can be partitioned into pairs $\left\{d, \frac{n^2+1}{d}\right\}$, where $d < \dfrac{n^2+1}{d}$. Clearly d is odd and less than n. Hence we have at most $\dfrac{n}{2}$ pairs, consequently $d(n^2+1) \leq n$.

Assuming to the contrary that the sequence becomes strictly monotonic starting with an N, it's obvious that it must be increasing (otherwise $d(n^2+1)$ would be forced to take negative values from some point $n > N$ onwards). Note that since n^2+1 is not a perfect square for any $n > 0$, hence $d(n^2+1)$ is an even number for every positive integer n. Since $d(n^2+1)$ is strictly monotonic for $n \geq N$, we deduce

$$d((n+1)^2+1) \geq d(n^2+1) + 2.$$

A straightforward induction proves that

$$d((n+k)^2+1) \geq d(n^2+1) + 2k. \tag{2.55}$$

By the inequality established in the beginning of the solution, for $N+t$ even we obtain the inequalities

$$N + t > d((N+t)^2+1) \geq d(N^2+1) + 2t, \tag{2.56}$$

or

$$N > d(N^2+1) + t \tag{2.57}$$

for any $t > 0$ which is impossible, since the rest of the terms of the inequality are constant. □

AFTERTHOUGHTS 2.5.1. *It must be mentioned that the problem was proposed for the Elemination Round of Saint-Peterburg Mathematical Olympiad in 1998 for 11th grade. The problem's author is A. Golovanov. Only 2 contestants solved the problem at the contest.*

Solution for (b). Note that since the sequence is not required to be strictly monotonic, we cannot infer that it will grow very fast, so the argument used at (a) fails. We will prove the following generalization:

Claim 2.5.1. *Let t and m be two positive integers. Then the sequence $d((n^2+m^2)^t)$ does not become monotonic from any given point onwards.*

Suppose, to the contrary, that from some point onwards, the sequence becomes monotonic. We will firstly show that it must be increasing. Indeed, take a prime p of the form $4k+1$. Clearly

-1 is a quadratic residue $\pmod p$, hence so is $-m^2$, so there is an integer r so that $p|r^2+m^2$. Take now d different primes $s_1,\ldots,s_d$ of the form $4u+1$ and let $r_i\in\mathbb{Z}$ so that $s_i \mid r_i^2+m^2$. Using the Chinese Remainder Theorem there is an integer N, so that $N\equiv r_i \pmod{s_i}$, for every $i=1,\ldots,d$. Then $N^2+m^2\equiv r_i^2+m^2 \pmod{s_i}$, hence $s_1\ldots s_d|N^2+m^2$. This implies that $d((N^2+m^2)^t)$ is unbounded, consequently it must be increasing from some point x_0 onwards.

For shortness of notations let $f_n=f(n)=d((n^2+m^2)^t)$. We will use the following very simple result.

Lemma 2.5.1. $\gcd(a^2+m^2,(a-1)^2+m^2)=1$ *if* $\gcd(2a-1,4m^2+1)=1$.

Proof. Let $\gcd(2a-1,4m^2+1)=1$ and suppose there is a prime p dividing both a^2+m^2 and $(a-1)^2+m^2$. By subtraction, we obtain $p|2a-1$. Then $2a\equiv 1 \pmod p$, so $4a^2\equiv 1 \pmod p$, or $4a^2+4m^2\equiv 1+4m^2 \pmod p$. Since $p\mid 4(a^2+m^2)$ we obtain $0\equiv 1+4m^2 \pmod p$, contradicting $\gcd(2a-1,4m^2+1)=1$. □

Take $x>x_0$ so that $\gcd(2x-1,1+4m^2)=1$. Then from LEMMA 2.5.1 and the identity $[x^2+m^2][(x-1)^2+m^2]=(x^2-x+m^2)^2+m^2$ we get the inequality $f_{x-1}f_x\le f_{x^2-x+m^2}$, since $d(uv)=d(u)\cdot d(v)$ if $\gcd(u,v)=1$.

We now state the following result, which we are going to use a bit later.

Lemma 2.5.2. *Let M be an integer. Then there exists a positive integer λ so that the polynomial $h(x)=4x^2-\lambda$ satisfies*

$$\gcd(2h(x)+1,M)=1,\forall x\in\mathbb{Z} \tag{2.58}$$

Proof. Since $2h(x)+1$ is odd, we need only prove the lemma for odd M. So assume M is odd and let $\{b_1,\ldots,b_s\}$ be the set of prime divisors of M. We are looking for λ so that $b_i \not| 2h(x)+1=8x^2-2\lambda+1$, $\forall i=\overline{1,s}$. Since b_i's are odd, the last condition is equivalent to $b_i \not| (4x)^2-(4\lambda-2)$. It is enough to find a λ so that $4\lambda-2$ is a quadratic nonresidue $\pmod{b_i}$. For every prime b_i there exists a quadratic non-residue r_i (actually there are $\dfrac{b_i-1}{2}$ of them). We will apply once again the Chinese Remainder Theorem in the following way:
We are looking for an integer L satisfying the following system of equations:

$$L\equiv r_i \pmod{b_i},\forall i=\overline{1,s} \tag{2.59}$$

$$L\equiv 2 \pmod 4 \tag{2.60}$$

and take $\lambda=\dfrac{L-2}{4}$. Clearly we can assume $\lambda>0$. □

Let's continue with the problem. Take $M=1+4m^2$ in LEMMA 2.5.2 to obtain such λ and $h(x)$. Using the monotonicity of f we deduce the chain of inequalities

$$f_{x-1}^2\le f_{x-1}f_x\le f_{x^2-x+m^2}\le f_{4(x-1)^2-\lambda},$$

for sufficiently large $x>x_0$. Here, we may also assume that x_0 is sufficiently large so that $x>x_0$ guarantees that $h(x)>x_0$. Note that the inequality $f_{x-1}f_x\le f_{x^2-x+m^2}$ provides another proof

that if f is monotonic, then it must be increasing. Hence ${f_q}^2 \leq f_{h(q)}$, where $q = x - 1 \geq x_0$, and $\gcd(2q+1, 1+4m^2) = 1$. Because by LEMMA 2.5.2 we have $\gcd(2h(q)+1, 4m^2+1) = 1$ we further get $f(q)^4 \leq \{f(h(q))\}^2 \leq f[h(h(q))]$. By an easy induction we obtain the inequalities

$$f(q)^{2^k} \leq f\left(\underbrace{h(h(\ldots h(q)\ldots))}_{k \text{ times}}\right) \leq f\left[(4q)^{2^k}\right]. \tag{2.61}$$

Here we have iteratively used the fact that $h(z) < 4z^2$. We are going now to summarize the obtained results. Let $c = f(q)$ and define $g(z)$ to be the positive integer satisfying

$$(4q)^{2^{g(z)}} \leq z < (4q)^{2^{g(z)+1}}. \tag{2.62}$$

We easily obtain $g(z) = \lfloor \log_2 \lfloor \log_{4q} z \rfloor \rfloor$. Then the above inequality and the monotonicity of f implies

$$c^{2^{g(z)}} \leq f(z) \tag{2.63}$$

for sufficiently large z. With this, we have found a lower estimate for $f(z)$.

Let's find an upper estimate for $f(x)$ which would contradict, for large enough x the lower estimate obtained above. For this, let $(p_i)_{i\geq 1}$ be the sequence of prime numbers, *not containing* the prime divisors of m. Let's take a closer look at $f(p_1 \ldots p_k)$. Let $(p_1 \ldots p_k)^2 + m^2 = \prod_{i=1}^{s} q_i^{\alpha_i}$. Using divisibility arguments, we have $q_i > p_j$ for all $i = \overline{1,s}$ and $j = \overline{1,s}$. This clearly implies $\sum_{i=1}^{s} \alpha_i \leq 2k$. Note that

$$f(p_1 \cdots p_k) = d\left(\left[(p_1 \ldots p_k)^2 + m^2\right]^t\right) = (t\alpha_1 + 1)\ldots(t\alpha_s + 1) =_{\text{def}} h(\alpha_1, \ldots, \alpha_s) \tag{2.64}$$

Using the already stated inequality $\sum_{i=1}^{s} \alpha_i \leq 2k$ we will prove that $h(\alpha_1, \ldots, \alpha_s) \leq (t+1)^{2k}$.

Indeed, note that if $a > 1$ then $(t+1)(t(a-1)+1) \geq ta + 1$. Hence if there is some $\alpha_i > 1$, Without Loss Of Generality, $\alpha_1 > 1$, we have $h(\alpha_1, \alpha_2, \ldots, \alpha_s) \leq h(\alpha_1 - 1, \alpha_2, \ldots, \alpha_s, 1)$. By repeated applications of this inequality until $\alpha_i = 1$, for all i, we obtain the following inequality

$$f(p_1 \cdots p_k) = h(\alpha_1, \ldots, \alpha_s) \leq h\left(\underbrace{1, 1, \ldots, 1}_{\sum \alpha_i}\right) \leq (t+1)^{\sum \alpha_i} \leq (t+1)^{2k} = T^k, \tag{2.65}$$

where $T = (t+1)^2$. Define now the function $l(x)$ to be equal $v+1$, where v is the unique positive integer for which $p_1 \ldots p_v < x \leq p_1 \ldots p_{v+1}$. Using once again the monotonicity of f, we establish the following upper bound for the function f:

$$f(x) \leq f\left(p_1 \ldots p_{l(x)}\right) \leq T^{l(x)} \tag{2.66}$$

Now, since $g(x) = \lfloor \log_2 \lfloor \log_{4q} x \rfloor \rfloor$, we have $g(x) > \log_2 \lfloor \log_{4q} x \rfloor - 1$, hence

$$2^{g(x)} > 2^{\log_2 \lfloor \log_{4q} x \rfloor - 1} = \frac{1}{2} \lfloor \log_{4q} x \rfloor. \tag{2.67}$$

It thus follows that

$$T^{l(x)} \geq f(x) \geq c^{2^{g(x)}} > \sqrt{c}^{\lfloor \log_{4q} x \rfloor}. \tag{2.68}$$

By the fact that f is unbounded, we can choose c as large as we want, hence we can assume $\sqrt{c} > T^2$. Then, for reaching a contradiction, we will show that $l(x) < 2\lfloor \log_{4q} x \rfloor$ for large enough x. Since $1 + \log_{4t} x < -2 + 2\log_{4t} x < 2\lfloor \log_{4t} x \rfloor$ for $\log_{4q} x > 3$, it is sufficient to prove $l(x) - 1 < \log_{4q} x$ for large enough x. The last inequality is equivalent to $(4q)^{l(x)-1} < x$. Recall that $4q$ is a constant value. We find that the primes grow very fast so that the inequality $(4q)^{l(x)-1} < p_1 \dots p_{l(x)-1}$ holds for large enough x. By the definition of $l(x)$, we have then, indeed, $p_1 \dots p_{l(x)-1} < x$, obtaining $l(x) - 1 < \log_{4q} x$, what we wanted.

□

AFTERTHOUGHTS 2.5.2 (About the sequence $\{p_i\}_{i\geq 1}$)**.** *We omitted proof of the validity of the above inequality $(4q)^{l(x)-1} < p_1 \dots p_{l(x)-1}$ for large enough x. Our sequence $\{p_i\}_{i\geq 1}$, though not equal to the sequence of prime numbers $\{P_i\}_{i\geq 1}$, is obtained from the set P of all primes by removing a finite number of primes - those dividing m, hence when x goes to ∞ it behaves just as P does.*

AFTERTHOUGHTS 2.5.3. *A polynomial $f \in \mathbb{Z}[X]$ is called a Bouniakowsky Polynomial if f is irreducible,* $\deg f > 1$ *and* $\gcd(f(1), f(2), \dots)) = 1$.

Theorem 2.5.1 (Bouniakowsky Conjecture)**.** *A Bouniakowsky polynomial takes prime values for infinitely many valuos of x.*

If the Bouniakowsky Conjecture is true, then we can easily prove that $d((n^2+1)^t)$, where t is a fixed positive integer, doesn't eventually become monotonic. Indeed, assume the contrary and suppose $d((n^2+1)^t)$ is monotonic from some point $n \geq n_0$. If the Conjecture is true, $n^2+1 > n_0$ is a prime for infinitely many values of n. For such values, $n^2+1 = p$, and $d((n^2+1)^t) = d(p^t) = t+1$. This, together with the monotonicity of the sequence would imply that $d((n^2+1)^t) \leq t+1$, $\forall n \geq n_0$. However we have proven before that n^2+1 can have an arbitrarily large number of divisors.

REFERENCES

1 S. L. Berlov, S. V. Ivanov, K. P. Kohasi, *St. Peterburg Mathematical Olympiads*

2.6 Vieta-Jumping

6 (IMO 1988/6) Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that

PEN A3

$$\frac{a^2+b^2}{ab+1} \tag{2.69}$$

is the square of an integer.

[PEN A4] (CRUX, Problem 1420, Shailesh Shirali) If a, b, c are positive integers such that

$$0 < a^2+b^2-abc \leq c, \tag{2.70}$$

show that a^2+b^2-abc is a perfect square.

Solution. Suppose that a, b are positive integers so that $ab+1$ divides a^2+b^2 and let

$$k := \frac{a^2+b^2}{ab+1}. \tag{2.71}$$

We have to prove that k is a perfect square. The very fundamental idea of this and similar problems is to give up the idea of proving properties of a and b directly. Instead, we are going to prove the desired property of k (i.e. that k is a perfect square) by fixing k and considering all positive integers a, b which satisfy $k = \frac{a^2+b^2}{ab+1}$, that is, we consider

$$S(k) := \left\{(a,b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : \frac{a^2+b^2}{ab+1} = k\right\}. \tag{2.72}$$

By defining this set, we leave the concrete values of a, b and instead take the whole 'environment' of k into consideration.

The next step is to assume the required statement to be wrong (for the sake of contradiction), that is, we suppose that k is not a perfect square. The rest of the problem goes by the method of *Infinite Descent*: We take any pair $(a,b) \in S(k)$ and show the existence of another pair $(a_1, b_1) \in S(k)$ which is smaller than (a,b) where (a_1, b_1) is said to be smaller than (a,b) if $a_1 + b_1 < a + b$. This however is a contradiction because $S(k) \subset \mathbb{Z}^+ \times \mathbb{Z}^+$ implies that there exists a lower bound for $a+b$ which is also achieved by at least one pair $(a,b) \in S(k)$.

Suppose that $(a,b) \in S(k)$ is any pair which satisfies $k = \frac{a^2+b^2}{ab+1}$. Wlog assume that $a \geq b$. Consider the equation

$$\frac{x^2+b^2}{xb+1} = k \tag{2.73}$$

as a quadratic equation in x. This equation is equivalent to

$$x^2 - kxb + b^2 - k = 0. \tag{2.74}$$

We know that $x = a$ is a root of $x^2 - kxb + b^2 - k = 0$ since $x = a$ solves $\frac{x^2+b^2}{xb+1} = k$. Let a_1 be the other solution of $x^2 - kxb + b^2 - k = 0$. Notice that by using the fact that this quadratic equation

has another solution, we have found another pair (a_1, b) that solves $\frac{x^2+b^2}{xb+1} = k$. The first step is to show that $(a_1, b) \in S(k)$.

Lemma 2.6.1. *a_1 is a positive integer.*

Proof. We know from Vieta's theorem that $a_1 = kb - a$. Thus, a_1 is an integer. We still have to prove that a_1 is positive. First, assume that $a_1 = 0$. But this implies that $k = b^2$ since we know that $x = a_1$ solves the equation $\frac{x^2+b^2}{xb+1} = k$, a contradiction to our assumption that k is not a perfect square. Now, assume that $a_1 < 0$. Then from $x^2 - kxb + b^2 - k = 0$ we infer that

$$k = a_1^2 - ka_1b + b^2 \geq a_1^2 + kb + b^2 > k, \tag{2.75}$$

clearly impossible. Notice that the last step follows from $b > 0$. We therefore know that $a_1 > 0$ and thus $a_1 \in \mathbb{Z}^+$. □

Corollary 2.6.1. *$(a_1, b) \in S(k)$.*

We hence have constructed another pair in $S(k)$ from any given pair (a, b). If we are able to prove that this new pair is smaller than the old one, we can use the argument of infinite descent to reach our contradiction and we are done. The next step is to prove that the new pair is indeed smaller than (a, b).

Lemma 2.6.2. *$a_1 < a$.*

Proof. We know that $x = a$ and $x = a_1$ are the roots of $x^2 - kxb + b^2 - k = 0$. It therefore follows from Vieta's theorem that

$$a_1 = \frac{b^2 - k}{a}. \tag{2.76}$$

However, since we assumed that $a \geq b$, we infer that

$$\frac{b^2 - k}{a} < a \tag{2.77}$$

from which $a_1 < a$ follows. □

We thus have proved the existence of a pair $(a_1, b_1) \in S(k)$ that is smaller than (a, b), i.e. that $a_1 + b_1 < a + b$. Iterating this procedure for (a_1, b_1), we can construct another pair $(a_2, b_2) \in S(k)$ that is smaller than (a_1, b_1) and another pair $(a_3, b_3) \in S(k)$ that is smaller than (a_2, b_2) and so on. In other words, we can construct pairs (a_j, b_j) for $j = 1, 2, \ldots$ so that

$$a + b > a_1 + b_1 > a_2 + b_2 > a_3 + b_3 > \ldots \tag{2.78}$$

which is impossible since all $(a_j, b_j) \in S(k) \subset \mathbb{Z}^+ \times \mathbb{Z}^+$. □

Revising this method, we first assumed the existence of a pair (a, b) that does not satisfy the statement we want to prove. We then went away from this concrete pair (a, b) and instead considered pairs with the same property as (a, b). The next step is to define a "size" of a pair (a, b) which in our case was simply $a + b$. It is trivial that this size has a lower bound. Using the theorem of Vieta, we constructed another pair (a_1, b_1) from any given pair (a, b) and we proved that the new pair is smaller than the old one. This method is called *Vieta-Jumping* or *Root Flipping*. Applying

the method of infinite descent, we obtain our desired contradiction.

With the same ideas, we can also prove A4:

[PEN A4] (CRUX, Problem 1420, Shailesh Shirali) If a, b, c are positive integers such that

$$0 < a^2 + b^2 - abc \leq c, \tag{2.79}$$

show that $a^2 + b^2 - abc$ is a perfect square.

Indeed, the first problem is a special case of this one since

$$0 < a^2 + b^2 - abc = c \tag{2.80}$$

implies that

$$\frac{a^2 + b^2}{ab + 1} = c \tag{2.81}$$

which must be a perfect square.

Solution. Again, as in the first problem, we assume that there exist positive integers a, b, c so that

$$k := a^2 + b^2 - abc \tag{2.82}$$

is not a perfect square. We know that $k > 0$ and $k \leq c$. We now fix k and c and consider all pairs (a, b) of positive integers which satisfy the equation $k = a^2 + b^2 - abc$, that is, we consider

$$S(c, k) = \left\{(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : a^2 + b^2 - abc = k\right\}. \tag{2.83}$$

Suppose that (a, b) is any pair in $S(c, k)$. Wlog assume that $a \geq b$. Consider the equation

$$x^2 - xbc + b^2 - k = 0 \tag{2.84}$$

as a quadratic equation in x. We know that $x = a$ is a root of this equation. Let a_1 be the other root of this equation.

Lemma 2.6.3. *a_1 is a positive integer.*

Proof. Since a_1 and a are the roots of $x^2 - xbc + b^2 - k = 0$, we know from the theorem of Vieta that

$$a_1 = bc - a. \tag{2.85}$$

It therefore follows that a_1 is an integer. If $a_1 = 0$ then $x^2 - xbc + b^2 - k = 0$ implies that $b^2 = k$ is a perfect square, a contradiction. If $a_1 < 0$ then $x^2 - xbc + b^2 - k = 0$ implies that

$$k = a_1^2 + b^2 - a_1 bc \geq a_1^2 + b^2 + bc > c, \tag{2.86}$$

a contradiction to $k \leq c$. Thus, a_1 is a positive integer. □

Corollary 2.6.2. $(a_1, b) \in S(c, k)$.

Again, it remains to be proven that the new pair (a_1, b) is smaller than (a, b).

Lemma 2.6.4. $a_1 < a$.

Proof. We know that a_1 and a are the roots of $x^2 - xbc + b^2 - k = 0$, so by Vieta's theorem,

$$a_1 = \frac{b^2 - k}{a}. \tag{2.87}$$

Since we assumed that $a \geq b$, it follows that

$$\frac{b^2 - k}{a} < a \tag{2.88}$$

which implies $a_1 < a$. □

We have therefore constructed another pair (a_1, b_1) in $S(c, k)$ with $a_1 + b_1 < a + b$. However, $S(c, k) \subset \mathbb{Z}^+ \times \mathbb{Z}^+$, so using the argument of infinite descent, we obtain our desired contradiction. □

Remark: There exists a bunch of problems which can be solved with these ideas. Here are some of them:

1. (IMO 2007/5) Let a, b be positive integers so that $4ab - 1$ divides $(4a^2 - 1)^2$. Show that $a = b$.

   Hint: First prove that if $4ab - 1 | (4a^2 - 1)^2$, then $4ab - 1 | (a - b)^2$.

2. (A5) Let x and y be positive integers such that xy divides $x^2 + y^2 + 1$. Show that

$$\frac{x^2 + y^2 + 1}{xy} = 3. \tag{2.89}$$

3. Let a, b be positive integers with $ab \neq 1$. Suppose that $ab - 1$ divides $a^2 + b^2$. Show that

$$\frac{a^2 + b^2}{ab - 1} = 5. \tag{2.90}$$

2.7 A Combinatorial Congruence

7 (Putnam 1991/B4) Suppose that p is an odd prime. Prove that

PEN D2

$$\sum_{j=0}^{p}\binom{p}{j}\binom{p+j}{j}\equiv 2^p+1 \pmod{p^2}.$$

First Solution. We first offer three well-known properties on binomial coefficients.

Lemma 2.7.1. *Let $\boldsymbol{p}$ be a prime and let $\boldsymbol{k}\in\{1,\cdots,p-1\}$. Then, we have*

$$\begin{cases} (\boldsymbol{a}) & \binom{p}{k}\equiv 0\ (mod\ p), \\ (\boldsymbol{b}) & \binom{p+k}{k}\equiv 1\ (mod\ p), \\ (\boldsymbol{c}) & \binom{2p}{p}\equiv 2\ \left(mod\ p^2\right). \end{cases} \tag{2.91}$$

Proof. For (**a**) and (**b**), we work on the field $\mathbb{Z}/p\mathbb{Z}$, also denoted as $\mathbb{Z}_p$, and identify the coset $\overline{a}=a+p\mathbb{Z}$ with $a\in\mathbb{Z}$. We compute

$$(\mathbf{a})\quad \binom{p}{k}=\binom{\overline{p}}{\overline{k}}\cdot\binom{p-1}{k-1}=\binom{\overline{0}}{\overline{k}}\binom{p-1}{k-1}=0, \tag{2.92}$$

and

$$(\mathbf{b})\quad \binom{p+k}{k}=\frac{(p+k)!}{k!p!}=\frac{1}{k!}\prod_{i=1}^{k}(p+i)=\frac{1}{k!}\prod_{i=1}^{k}i=\frac{1}{k!}k!=1. \tag{2.93}$$

It follows from Vandermonde's Identity and (**a**) that

$$(\mathbf{c})\quad \binom{2p}{p}\equiv\sum_{k=0}^{p}\binom{p}{k}\binom{p}{p-k}\equiv 1+\sum_{k=1}^{p-1}\binom{p}{k}^2+1\equiv 2\left(mod\ \mathbf{p}^2\right). \tag{2.94}$$

□

Now, we prove the congruence in the problem. By (**a**) and (**b**) in LEMMA 12, whenever $j\in\{1,\cdots,p-1\}$, the integer $\left(\binom{p+j}{j}-1\right)\binom{p}{j}$ is divisible by p^2, in other words, $\binom{p}{j}\binom{p+j}{j}\equiv\binom{p}{j}\ \left(mod\ p^2\right)$.

It follows from the above, LEMMA 12 and the BINOMIAL THEOREM that

$$\begin{aligned}\sum_{j=0}^{p}\binom{p}{j}\binom{p+j}{j} &\equiv 1+\left(\sum_{j=1}^{p-1}\binom{p}{j}\binom{p+j}{j}\right)+\binom{2p}{p} \pmod{p^2}\\ &\equiv 1+\sum_{j=1}^{p-1}\binom{p}{j}+2 \pmod{p^2}\\ &\equiv 1+(2^p-2)+2 \pmod{p^2}\\ &\equiv 2^p+1 \pmod{p^2}.\end{aligned}$$

□

Second Solution. We establish the following combinatorial identity.

Lemma 2.7.2. *For all positive integers* $\boldsymbol{n}$*, we have*

$$\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}=\sum_{k=0}^{n}\binom{n}{k}^2 2^k. \tag{2.95}$$

Proof. We first expand the polynomial $(2+x)^n(1+x)^n = ((1+x)+1)^n(1+x)^n$ in two ways. On the one hand, we compute

$$f(x)=\left(\sum_{k=0}^{n}\binom{n}{k}2^k x^{n-k}\right)\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right)=\sum_{l=0}^{2n}\left(\sum_{k+j=l,0\le k,j\le n}\binom{n}{k}\binom{n}{j}2^k\right)x^l. \tag{2.96}$$

On the other hand, we compute

$$\begin{aligned} f(x) &= \left(\sum_{k=0}^{n}\binom{n}{k}(1+x)^k\right)(1+x)^n \\ &= \sum_{k=0}^{n}\binom{n}{k}(1+x)^{n+k} \\ &= \sum_{k=0}^{n}\binom{n}{k}\left(\sum_{j=0}^{n+k}\binom{n+k}{j}x^j\right) \\ &= \sum_{j=0}^{2n}\left(\sum_{k=max(0,n-j)}^{n}\binom{n}{k}\binom{n+k}{j}\right)x^j \end{aligned}$$

□

Now, we can find the coefficient of x^n in $f(x)$ in two ways. The first identity gives

$$x^n[f(x)]=\sum_{k+j=n}\binom{n}{k}\binom{n}{j}2^k=\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}2^k=\sum_{k=0}^{n}\binom{n}{k}^2 2^k \tag{2.97}$$

and the second identity gives

$$x^n[f(x)]=\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{n}=\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}. \tag{2.98}$$

Equating the coefficients $x^n[f(x)]$, we get the desired result.

Now, we go back to the original problem. We take $n=p$ in LEMMA 12 and use the fact that $\binom{p}{k}$ is divisible by $\mathbf{p}$(established in the previous offered solution), where $k\in\{1,\cdots,p-1\}$. We obtain

$$\sum_{j=0}^{p}\binom{p}{j}\binom{p+j}{j}\equiv 1+\sum_{j=1}^{p-1}\binom{p}{j}^2 2^j+2^p\equiv 1+2^p \pmod{p^2}. \tag{2.99}$$

□

2.8 An arithmetic partition

8 (Romania TST 1998) Let n be a prime and $a_1 < a_2 < \ldots < a_n$ be integers. Prove that $a_1, a_2, \ldots, a_n$ is an arithmetic progression if and only if there exists a partition of $\mathbb{N}_0 = \{0, 1, 2, \ldots, \}$ into n sets $A_1, A_2, \ldots, A_n$ so that

PEN O35

$$a_1 + A_1 = a_2 + A_2 = \ldots = a_n + A_n, \tag{2.100}$$

where $x + A = \{x + a | a \in A\}$.

Vasile Pop

First Solution. Assume firstly that $a_1, a_2, \ldots, a_n$ is an arithmetic progression. Define $A_i = \{knr + ir + j | k \in \mathbb{N}_0, 0 \leq j \leq n-1\}$. It is easy to see that $\mathbb{N}_0 = A_1 \cup A_2 \ldots \cup A_n$ and $A_i \cap A_j = \emptyset$ for $i \neq j$.

The converse part is much more difficult. For convenience of notations, let $B_i = A_{n-i}$ and $r_i = a_n - a_{n-i}$. Hence $B_i = B_0 + r_i$ and $\mathbb{N}_0 = B_0 \cup B_1 \cup \ldots \cup B_{n-1}$. Call a segment of length k of a subset B_i a set $S \subset B_i$ of the form $\{m+1, \ldots, m+k\}$, where $m, m+k+1 \notin B_i$.

Lemma 2.8.1. *Any segment of any subset B_i has length $r = r_1$.*

Proof. Note that if B_i for some $i > 0$ contains a segment of length different from r, then so must B_0, since $B_i = B_0 + r_i$. Hence it is enough to show that B_0 consists only of segments of length r. Indeed, note that if $m \in B_0$ then $m + r \in B_1$, hence any segment of B_0 has length at most r. Assume to the contrary that there is at least one segment of length less than r in B_0. Among all such segments, let $S = \{m+1, \ldots, m+k\} \subset B_0$ with $k < r$ be the one with smallest m (the 'first' one). Then $\{m+1+r, m+2+r, \ldots, m+k+r\}$ is a segment of B_1. Since $m+k+1 \notin B_0$, $m + r \notin B_1$, and the set $\{m+k+1, \ldots, m+r\}$ has $r - k > 0$ elements it follows that there is a segment $T \subset \{m+k+1, \ldots, m+r\}$ of some B_i, $i > 0$ of length at most $r - k$. Hence $T - r_i = \{m+k+1-r_i, \ldots, m+r-r_i\}$ is a segment of length at most $r - k < r$ of B_0. Since $m + k + 1 - r_i < m$, this contradicts the definition of S. □

Lemma 2.8.2. *Each B_i starts with the segment $S_i = \{ir, ir+1, \ldots, ir+r-1\}$.*

Proof. We prove the statement by induction on i. It is clear that $S_0 = \{0, 1, \ldots, r-1\} \subset B_0$, which is the base of our induction. Assume the statement true for $0 \leq i < k$. We are going to show the statement for $i = k$.

So $S_i \subset B_i$, $i = \overline{0, k-1}$. Let $S_k \subset B_j$ and assume, to the contrary, that $j \neq k$. From $a_1 < a_2 < \ldots < a_n$ we get $r_1 < r_2 < \ldots < r_n$. This implies $j < k$. But then S_k is already the second segment of B_j (after S_j) which is impossible for $j > 0$, since we haven't reached the second segment of B_0 yet. Hence $j = 0$, and so $S_k \in B_0$. Note that for $j < k$ we have $r_j = jr$. Then it follows that $S_i \subset B_{i-k}$ for $i = k, k+1, \ldots, 2k-1$. Again, S_{2k} must be a subset of either B_0 or B_k. If $S_{2k} \subset B_0$ then we apply the above argument again to obtain $S_i \in B_{i-2k}$ for $i = 2k, 2k+1, \ldots, 3k-1$. Repeating this process, we obtain that the first segment of B_k must be

of the form S_{tk}, for some t. This implies $r_k = tk$.

Let's prove now by induction on l, that if $lk < n$ then each apparition of a segment from B_{lk} is followed by a sequence of segments belonging to the sets $B_{lk+1}, \ldots, B_{lk+-1}$, implying that $(l+1)k \leq n$. Moreover, if $(l+1)k \leq n$ then the first segment of $B_{(l+1)k}$ is of the form S_{tk} for some t.

For $l = 0$ the statement of trivial. Assume now the statement true for all $l < u$ and let's prove it for $l = u$. Assume $lk < n$. Applying the inductive hypothesis for $l = u - 1$, we get that the first segment of $B_{(u+1)k} = B_{lk}$ is of the form S_{tk} for some t. Take the segment S_{tk+i}, $0 < i < k$. Let's prove that it belongs to a new segment B_{lk+i}. Indeed assume $S_{tk+i} \in B_j$ for some j. Assume B_j has appeared before. The inductive hypothesis shows that each B_{xk+i}, $x < l$, $0 \leq i < k$ has only segments of the form $S_{x'k+i}$, for some x'. Hence $r_{xk+i} = Mrk + ri$, for some M. Also, the inductive hypothesis shows that $r_{xk} + ri = r_{xk+i}$, $0 \leq i < k$. It follows that $j = t'k + i$, for some $t' < l$ and that $r_{t'k} = r_j - ri$. Since $S_{tk+i} \in B_j$ has been obtained by adding r_j to some segment $S_{hk} \in B_0$, it follows that when adding $r_{t'k} = r_j - ri$ to S_{hk} we should obtain a segment belonging to $B_{t'k}$. However $S_{hk} + r_j - r_i = S_{tk+i} - ri = S_{tk} \in B_{lk}$. Contradiction because $t' < l$.

From the last result, we infer that $k|n$, which is impossible for $1 < k < n$. Hence the proof of LEMMA 2.8.2 is completed. □

LEMMA 2.8.2 states that $S_i \subset B_i$, for $i = 0, 1, \ldots, n-1$, hence $r_i = ir$ for all i, implying that $a_1, a_2, \ldots, a_n$ is an arithmetic progression with term difference r. □

Second Solution. If $a_1, \ldots, a_n$ is an arithmetic progression, proceed like in the previous solution. Let's prove the converse. Again, let $B_i = A_{n-i}$ and $r_i = a_n - a_{n-i}$, hence $B_i = B_0 + r_i$. Let $f(m, i)$ be the number of nonnegative integers $\leq m$ which are in B_i. Clearly $f(m, i) = f(m - r_i, 0)$. Because the sets (B_i) cover the set of nonnegative integers, $m + 1 = f(m, 0) + f(m, 1) + \ldots + f(m, n-1)$. Define $x_i = f(i, 0)$ for $i \geq 0$ and $x_i = 0$ for $i < 0$. Using the above remark, we obtain

$$x_m + x_{m-r_1} + \ldots + x_{m-r_{n-1}} = m + 1, \tag{2.101}$$

for $m \geq 0$. Adding the above relation for $m - 1$, $m + 1$ and subtracting it twice for m, we obtain

$$t_m + t_{m-r_1} + \ldots + t_{m-r_{n-1}} = 0, \tag{2.102}$$

where $t_i = x_{i+1} + x_{i-1} - 2x_i$.

From the definition of t_i and x_i we observe that $t_i \in \{-1, 0, 1\}$. This and the recurrence relation for the sequence (t_i) implies that (t_i) is a periodic sequence. Let M be the length of its smallest period. Then $t_{i+1} + t_{i+2} + \ldots + t_{i+M}$ is a constant value. Let's prove that this value equals 0. Indeed, let $C = t_{i+1} + t_{i+2} + \ldots + t_{i+M}$. Let N be a positive integer. Summing up the recurrence relation for $m = 0$ to N, we obtain

$$0 = n(t_0 + \ldots + t_{N-r_{n-1}}) + E, \tag{2.103}$$

where E consists of finitely many t_i's (for example, less than $(r_{n-1}+1)^2$ t_i's), hence it is bounded: $|E| < h$ for some constant h implying that $t_0 + \ldots + t_{N-r_{n-1}}$ is bounded for all N. On the other side $t_0 + \ldots + t_{kM-1} = kC$ as it is the sum of k blocks of t_i's. If $C \neq 0$ for large enough k we have $|kC| > h$. Impossible. So $C = 0$.

Since $t_{i+1} + \ldots + t_{i+M} = (x_i - x_{i+1}) - (x_{i+M} - x_{i+M+1}) = 0$, we have the implication: if $i \in B_0$ then $i + M \in B_0$. Moreover, if $i \in B_j$ then $i + M \in B_j$ for $j = \overline{0, n-1}$. Let B be the subset of B_0 having all elements less than M. Let's prove that

$$B \cup B + r_1 \cup \ldots \cup B + r_{n-1} = \{0, 1, \ldots, M-1\}. \tag{2.104}$$

It is obvious that every $m \in \{0, 1, 2, \ldots, M-1\}$ belongs to some $B + r_i$. For the converse, let $x = y + r_i$, for some $y \in B$. Assume, to the contrary, that $x \geq M$. Let $x = qM + r$, $q \geq 1$, $M - 1 \geq r \geq 0$. Then $r \in B + r_i$, hence $r - r_i \in B$, hence $r \geq r_i$. Since $y + r_i = qm + r \geq qm + r_i$, we obtain $y \geq qm \geq m$. Impossible since $y \in B$.

Denote now by R the set $\{0, r_1, \ldots, r_{n-1}\}$. Define set addition as $X + Y = \{x + y | x \in X, y \in Y\}$. We are to show that if $B + R = \{0, 1, \ldots, M-1\}$ and $|R|$ is a prime number, then $0, r_1, \ldots, r_{n-1}$ form an arithmetic progression. We will make use of the following Lemma, which proves better than anything the power of the Extremal Principle:

Lemma 2.8.3. *Let X and Y be two sets so that $X+Y = \{0, 1, \ldots, M-1\}$. Let $m = \min(Y \setminus \{0\})$. Then $|X|$ is a multiple of m and there exist sets X' and Y' so that $X' + Y' = \left\{0, 1, \ldots, \dfrac{M}{m} - 1\right\}$ and $X = mX' + \{0, 1, \ldots, m-1\}$, $Y = mY'$.*

Proof. Let's show firstly that every element of Y is a multiple of m. Indeed, note firstly that $\{0, 1, \ldots, m-1\} \subseteq X$. Note also that every element from $\{0, 1, \ldots |X| \cdot |Y| - 1\}$ can be uniquely written as $x+y$, where $x \in X$ and $y \in Y$. Assume to the contrary that there is an $y = qm+r \in Y$, with $0 < r < m$. Among all such numbers, take the one with smallest q. If $qm \in Y$, since $r \in X$ then $qm + r = (qm + r) + 0$ are two representations of the same number as $x + y$, $x \in X$, $y \in Y$. Impossible. Hence $qm \notin Y$. Also, $qm \notin X$, because otherwise $qm + m = (qm + r) + (m - r)$. Hence $qm \notin X, Y$. Since $qm < qm + r$ and all elements less than $qm + r$ in Y are multiples of m, we deduce the existence of a positive u so that $um \in Y$ and $(q - u)m \in X$. Let's prove now that: if $km \in X$ for some $k < q - u$ then $km + r \in X$, for all $0 < r < m$; and if $km + r \in X$ for some $0 < r < m; k < q - u$ then $km \in X$. Assume to the contrary that there is a pair (k, r) so that $km \in X$ and $km+r \notin X$ or $km \notin X$ and $km+r \in X$. Among all such pairs take the one with the smallest k. Assume firstly $km \in X$ and $km + r \notin X$. Consider the number $z = km + r$. By our choice $z \notin X$. By the minimality of q, we obtain $z \notin Y$, hence $z \notin X, Y$. Hence there is a positive $x < q$ such that $z = xm + (k - x)m + r$, where $xm \in Y$ and $(k - x)m + r \in X$. *By our choice of k and r, we have* $(k - x)m \in X$. Since $km \in X$ and $xm \in Y$, we obtain two distinct representations: $km = km + 0 = (k - x)m + xm$. Impossible. The second case is treated in an analogous way. Consider now the number $Z = (q - u)m + r$. If $Z \in X$, then $Z + um = (qm + r) + 0$, impossible. Also from the minimality of q, $Z \notin Y$. Hence there exist $x \in X$ and $y \in Y$ so that $Z = x + y$.

Because $Z < qm + r$, $x = tm$ for some $t > 0$, and $y = (q - u - t)m + r$. From what was proved above, we obtain that $(q - u - t)m \in X$. But then $(q - u - t)m + um = (q - u)m + 0$ are two distinct representations of $(q - u)m$ as sum $x + y$, $x \in X$ and $y \in Y$. Contradiction.

So every element of Y is a multiple of m and writing $Y = mY'$, for some set Y' makes sense. We'll now prove in a completely similar way as above that if $km \in X$ for some k, then $km + r \in X$, for $0 < r < m$; and conversely, if $km + r \in X$ for some $0 < r < m$, then $km \in X$. Among all such *bad* pairs, take the one with the least k. For the sake of completeness we shall now treat the second case. Assume that $km + r \in X$ for some $0 < r < m$ and that $km \notin X$. It is easy to see that $km \notin Y$, otherwise $km + r = (km + r) + 0$. Hence there is a positive x so that $xm \in Y$ and $(k - x)m \in X$. By the choice of our k, we obtain that $(k - x)m + r \in X$. But then $(km + r) + 0 = [(k - x)m + r] + xm$ are two distinct representations. Contradiction. So we can write $X = mX' + \{0, 1, \ldots, m - 1\}$.

It remains to prove that $X' + Y' = \left\{0, 1, 2, \ldots, \frac{M}{m} - 1\right\}$. Indeed, let $k \in \left\{0, 1, 2, \ldots, \frac{M}{m} - 1\right\}$ and take consider $z = km \in \{0, 1, \ldots, M - 1\}$. Since the representation $z = x + y$ in $X + Y$ is unique and $m|y$ we also have $m|x$, so the representation $k = x/m + y/m = x' + y'$ where $x' \in X'$, $y' \in Y'$ is unique. □

Note that LEMMA 2.8.3 is symmetrical with respect to X and Y.

Let's now finish the problem. We will prove by induction on $|B|$ that if $B \cup R = \{0, 1, \ldots, |B| \cdot |R| - 1\}$ then $0, r_1, \ldots, r_{n-1}$ form an arithmetic progression. If $|B| = 1$, then $B = \{0\}$ and $B + R = B = \{0, 1, \ldots, n - 1\}$ so $r_i = i$ and we are done. Assume now the statement true for all sets B having less than b elements. We have two cases:

If $1 \in R$, then $m = \min(B \setminus \{0\}) > 1$ and from Lemma 3, $m|n$. Since n is a prime number, it follows that $m = n$. Then it follows that $|R'| = 1$, $R' = \{0\}$, so $R = mR' + \{0, 1, \ldots, m - 1\} = \{0, 1, \ldots, m - 1\}$ and the statement is true.

If $1 \notin R$, then $m = \min(R \setminus \{0\}) = r_1|b$. By Lemma 3, $R = mR'$ and $B = mB' + \{0, 1, \ldots, m - 1\}$. R' and B' have the properties that $|R'| = |R|$ is a prime, $R' + B' = \{0, 1, \ldots, |R'| \cdot |B'| - 1\}$ and $|B'| = \frac{b}{m} < b$, hence by the induction hypothesis the elements of R' form an arithmetic progression. Because $R = mR'$ the same holds for $0, r_1, \ldots, r_{n-1}$. □

2.9 Primitive Roots: Revisited

9 Suppose that m does not have a primitive root. Show that

PEN B6

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m} \tag{2.105}$$

for every a relatively prime to m.

First, we use the well known fact that m has primitive roots if and only if m has the form $2, 4, p^k$ or $2p^k$ where p is an odd prime number and k is a positive integer. We thus have to prove the statement for all other numbers.

First Solution. First, notice that if m has no primitive roots and is not a power of 2, then we can write m as $m = m_1 m_2$ where m_1 and m_2 are positive integers satisfying $2 \mid \varphi(m_1)$ and $2 \mid \varphi(m_2)$. Since $a^{\varphi(m_1)} \equiv 1 \pmod{m)_1}$ for every integer a coprime to m_1 and $a^{\varphi(m_2)} \equiv 1 \pmod{m)_2}$ for every integer a coprime to m_2, we have

$$a^{\varphi(m_1)\frac{\varphi(m_2)}{2}} \equiv 1 \pmod{m_1} \tag{2.106}$$

and

$$a^{\varphi(m_2)\frac{\varphi(m_1)}{2}} \equiv 1 \pmod{m_2} \tag{2.107}$$

for every integer a coprime to $m_1 m_2 = m$. Thus, by the chinese remainder theorem, it follows that

$$a^{\frac{\varphi(m_1)\varphi(m_2)}{2}} = a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_1 m_2 = m} \tag{2.108}$$

which proves the proposition for all desired m that are not a power of 2.

Suppose now that $m = 2^k$ is a power of 2 and has no primitive roots. Notice that $k \geq 3$. The proof of the claim goes by induction on k. For $k = 3$, we can simply check that $a^{\frac{\varphi(8)}{2}} = a^2 \equiv 1 \pmod{8}$ for all odd a (we have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$). Suppose now that $a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$ for some positive integer $k \geq 3$ and every odd integer a. Then for every such a, we either have

$$a^{2^{k-2}} \equiv 1 \pmod{2^{k+1}} \tag{2.109}$$

or

$$a^{2^{k-2}} \equiv 1 + 2^k \pmod{2^{k+1}}. \tag{2.110}$$

In the first case, we trivially have

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \tag{2.111}$$

and in the second case, we have

$$\left(a^{2^{k-1}}\right)^2 \equiv \left(1 + 2^k\right)^2 \equiv 1 + 2^{k+1} + 2^{2k} \equiv 1 + 2^{2k} \pmod{2^{k+1}} \tag{2.112}$$

and since $k \geq 3$, we have $2k \geq k + 1$,

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \tag{2.113}$$

which proves the induction step. □

Second Solution. From a more advanced and more general point of view, we can analyze the smallest positive integer t, so that $a^t \equiv 1 \pmod{m}$ for every integer a coprime to m, where m is a given positive integer.

Definition 2.9.1. *Let m be a positive integer. Then $\lambda(m)$ denotes the least positive integer t so that*

$$a^t \equiv 1 \pmod{m} \tag{2.114}$$

holds for all integers a coprime to m. λ is called the Carmichael Function.

We start with an easy lemma:

Lemma 2.9.1. *Let m and t be positive integers. Then*

$$a^t \equiv 1 \pmod{m} \tag{2.115}$$

holds for every integer a coprime to m if and only if $\lambda(m) \mid t$. In particular, $\lambda(m) \mid \varphi(m)$.

Proof. The claim is trivial if $\lambda(m) \mid t$. On the other hand, if

$$a^t \equiv 1 \pmod{m} \tag{2.116}$$

holds for every integer a coprime to m, then by the integer division algorithm, there exist integers q and r so that $t = q\lambda(m) + r$ and $0 \leq r \leq \lambda(m) - 1$. Thus, for every integer a coprime to m, we have

$$1 \equiv a^t \equiv a^{q\lambda(m)+r} \equiv a^{q\lambda(m)} \cdot a^r \equiv a^r \pmod{m}. \tag{2.117}$$

But $r < \lambda(m)$ and since we have defined $\lambda(m)$ as the smallest positive integer with this property, this implies $r = 0$ and thus $\lambda(m) \mid t$. □

In order to solve the problem, we can derive a (well known) formula for $\lambda(m)$:

Proposition 2.9.1. *Let $m \geq 2$ be a positive integer. Then*

$$\lambda(m) = \begin{cases} \varphi(m) & \text{if } m = 2, 4, p^k, 2p^k \text{ where } p \text{ is an odd prime and } k \in \mathbb{Z}^+, \\ 2^{k-2} & \text{if } m = 2^k \text{ where } k \geq 3 \text{ is an integer}, \\ \operatorname{lcm}(\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r})) & \text{if } m = p_1^{k_1} \ldots p_r^{k_r} \text{ is the prime factorization of } m. \end{cases} \tag{2.118}$$

Proof. The first line directly follows from the existence of primitive roots modulo $m = 2, 4, p^k, 2p^k$. For the second one, we can, as in the first proof of this problem, first show that if $k \geq 3$ is an integer, then

$$a^{2^{k-2}} \equiv 1 \pmod{2^k} \tag{2.119}$$

for every odd integer a (which implies that $\lambda(2^k) \leq 2^{k-2}$. Next, we can show by induction on k that there exists an odd integer a which satisfies $\operatorname{ord}_{2^k}(a) = 2^{k-2}$ for every integer $k \geq 3$ (which implies the minimality of 2^{k-2}). This is clear if $k = 3$ or $k = 4$, simply take $a = 3$ for example and observe that $\operatorname{ord}_8(3) = 2$ and $\operatorname{ord}_{16}(3) = 4$. Suppose now that for some integer $k \geq 4$ and some odd integer a, we have

$$\operatorname{ord}_{2^{k-1}}(a) = 2^{k-3} \quad \text{and} \quad \operatorname{ord}_{2^k}(a) = 2^{k-2}. \tag{2.120}$$

This however implies that

$$a^{2^{k-3}} \equiv 1 \pmod{2^{k-1}} \quad \text{but} \quad a^{2^{k-3}} \not\equiv 1 \pmod{2^k}, \tag{2.121}$$

so

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k} \tag{2.122}$$

and thus, we either have

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^{k+1}} \tag{2.123}$$

or

$$a^{2^{k-3}} \equiv 1 + 2^{k-1} + 2^k \pmod{2^{k+1}}. \tag{2.124}$$

In the first case, we have

$$a^{2^{k-2}} \equiv \left(1 + 2^{k-1}\right)^2 \equiv 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \not\equiv 1 \pmod{2^{k+1}} \tag{2.125}$$

and in the second case, we have

$$a^{2^{k-2}} \equiv \left(1 + 2^{k-1} + 2^k\right)^2 \equiv 1 + 2^{2k-2} + 2^{2k} + 2^k + 2^{k+1} + 2^{2k} \equiv 1 + 2^k \not\equiv 1 \pmod{2^{k+1}}. \tag{2.126}$$

So in both cases, we have $a^{2k-2} \not\equiv 1 \pmod{2^{k+1}}$ and since $\mathrm{ord}_{2^{k+1}}(a) \mid \varphi(2^{k+1}) = 2^k$, we have $\mathrm{ord}_{2^{k+1}}(a) \geq 2^{k-1}$. But we already know that $\lambda(2^{k+1}) \leq 2^{k-1}$ and since $\mathrm{ord}_{2^{k+1}}(a) \leq \lambda(2^{k+1})$, this implies $\mathrm{ord}_{2^{k+1}}(a) = 2^{k-1}$ and thus $\lambda(2^{k+1}) = 2^{k-1}$. For the third one, we assume that $m = m_1 m_2$ where $m_1, m_2 > 1$ are coprime positive integers. Then by the chinese remainder theorem,

$$a^t \equiv 1 \pmod{m} \tag{2.127}$$

holds for every integer a coprime to m if and only if

$$a^t \equiv 1 \pmod{m_1} \tag{2.128}$$

holds for every integer a coprime to m_1 and

$$a^t \equiv 1 \pmod{m_2} \tag{2.129}$$

holds for every integer a coprime to m_2. However, by LEMMA 2.9.1, the latter holds if and only if

$$\lambda(m_1) \mid t \quad \text{and} \quad \lambda(m_2) \mid t \tag{2.130}$$

and since we have defined $\lambda(m)$ as the smallest smallest positive integer t which satisfies $a^t \equiv 1 \pmod{m}$ and thus the smallest positive integer satisfying $\lambda(m_1) \mid t \quad \text{and} \quad \lambda(m_2) \mid t$, we obtain

$$\lambda(m) = \mathrm{lcm}(\lambda(m_1), \lambda(m_2)). \tag{2.131}$$

□

From PROPOSITION 2.9.1, we immediately infer that

Corollary 2.9.1. *Let $m \geq 2$ be a positive integer. Then $\lambda(m) = \varphi(m)$ if and only if $m = 2, 4, p^k, 2p^k$ where p is an odd prime number and k is a positive integer. For all other m we have $\lambda(m) < \varphi(m)$ and since $\lambda(m) \mid \varphi(m)$ by* LEMMA 2.9.1*, we have $\lambda(m) \leq \varphi(m)/2$.*

It thus remains to be proven that if m has no primitive roots, then $\lambda(m) \mid \varphi(m)/2$. This is clear if $m \geq 8$ is a power of two. Otherwise, by PROPOSITION 2.9.1, we have at least two coprime divisors m_1 and m_2 with $\varphi(m_1), \varphi(m_2)$ being even, which implies that at least one factor 2 drops out of $\varphi(m)$ if compared to $\lambda(m)$. This solves the problem. □

2.10 Partitions

10 PEN O49 ((D. Fomin) [Ams, pp. 12]) Consider the set of all five-digit numbers whose decimal representation is a permutation of the digits $1, 2, 3, 4, 5$. Prove that this set can be divided into two groups, in such a way that the sum of the squares of the numbers in each group is the same.

Proof. For this problem, let us denote

$$\sigma : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\} : i \mapsto 6 - i$$

and

$$S = \{n \in \mathbb{N} | n > 33333 \text{ and } n \text{ is a digit permutation of } 12345\}. \tag{2.132}$$

Also, we will write $[a, b, c, d, e]$ for the number $10000a + 1000b + 100c + 10d + e$, and we define

$$[a, b, c, d, e]^\sigma := [\sigma(a), \sigma(b), \sigma(c), \sigma(d), \sigma(e)]. \tag{2.133}$$

Now, we can represent each number $s \in S$ as $s = [a, b, c, d, e]$, with $a, b, c, d, e \in \{1, 2, 3, 4, 5\}$ keeping in mind that $abcde > 33333$. We define the difference T_{abcde} as

$$T_{abcde} = [a, b, c, d, e]^2 - [\sigma(a), \sigma(b), \sigma(c), \sigma(d), \sigma(e)]^2, \tag{2.134}$$

which rewrites as $[6, 6, 6, 6, 6] \cdot [a - \sigma(a), b - \sigma(b), c - \sigma(c), d - \sigma(d), e - \sigma(d)]$. Also, observe that when $[a, b, c, d, e] > 33333$, then we automatically have $[\sigma(a), \sigma(b), \sigma(c), \sigma(d), \sigma(e)] < 33333$ and vice versa (since the sum is 66666), hence exactly half of our five-digit numbers are in S (and σ is a bijection between the elements in S and the elements in S^c, the complement of S.

Now consider the following problem: let T be the set

$$T := \{T_{abcde} | [a, b, c, d, e] \in S\}. \tag{2.135}$$

Prove that we can split T into two disjoint sets T_1, T_2 with equal sum of elements.

If we find such T_1, T_2, then

$$S_1 := \{[a, b, c, d, e] | [a, b, c, d, e] \in T_1\} \cup \{[a, b, c, d, e]^\sigma | [a, b, c, d, e] \in T_2\}$$

$$S_2 := \{[a, b, c, d, e] | [a, b, c, d, e] \in T_2\} \cup \{[a, b, c, d, e]^\sigma | [a, b, c, d, e] \in T_1\} \tag{2.136}$$

is a valid partition for our original problem.

That leaves us to find T_1, T_2. First observe that, if we define

$$\tau : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\} : (12)(3)(4)(5). \tag{2.137}$$

then $[a, b, c, d, e] > 33333$ if and only if $[a, b, c, d, e]^\tau := [\tau(a), \tau(b), \tau(c), \tau(d), \tau(e)] > 33333$, hence we can split the elements of T into pairs (t_1, t_2) with $t_1 > t_2$, where the only difference is the

switched positions of 1 and 2.

For $[a,b,c,d,e] > 33333$, we need $a \geq 3$, so the difference $t_1 - t_2 \in \{9, 90, 99, 900, 990, 999\}$, appearing respectively $3!, 3!, 3!, 3! - 2!, 3! - 2!, 3! - 2!$ times. To find our T_1, T_2, it is sufficient to partition the set of pairs (t_1, t_2) into two sets A and B such that

$$\sum_{(t_1,t_2)\in T_1} t_1 - t_2 = \sum_{(t_1,t_2)\in T_2} t_1 - t_2,$$

since this will cause them to have an equal sum over the elements in the set.

Now note that $999 = 990 + 9,\ 999 = 900 + 99,\ 990 = 900 + 90$ and $99 = 90 + 9$. Hence:

1. Put 3 pairs with $t_1 - t_2 = 999$ into A, 3 pairs with $t_1 - t_2 = 990$ into B, 3 pairs with $t_1 - t_2 = 9$ into B.
2. Put 3 pairs with $t_1 - t_2 = 999$ into A, 3 pairs with $t_1 - t_2 = 900$ into B, 3 pairs with $t_1 - t_2 = 99$ into B.
3. Put 3 pairs with $t_1 - t_2 = 990$ into A, 3 pairs with $t_1 - t_2 = 900$ into B, 3 pairs with $t_1 - t_2 = 90$ into B.
4. Put 1 pair with $t_1 - t_2 = 99$ into A, 1 pair with $t_1 - t_2 = 90$ into B, 1 pair with $t_1 - t_2 = 9$ into B.

By the counting above, we have partitioned all of the pairs into two sets, which have an equal sum over the elements per construction.

Now, we define

$$T_1 := \{t_1 | (t_1, t_2) \in A\} \cup \{t_2 | (t_1, t_2) \in B\}$$

and

$$T_2 := \{t_2 | (t_1, t_2) \in A\} \cup \{t_1 | (t_1, t_2) \in B\}.$$

Since A and B are partitions of the couples of elements of S, this is a valid partition. □