Problems in Elementary Number Theory

Volume 2, No. 1, Spring 2009

pen@problem-solving.be

Written by PEN Team

Andrei Frimu	Moldova
Yimin Ge	Austria
Daniel Kohen	Argentina
David Kotik	Canada
Hojoo Lee	Korea
Soo-Hong Lee	Korea
Cosmin Pohoata	Romania
Ho Chung Siu	Hong Kong
Peter Vandendriessche	Belgium
Ofir Gorodetsky	Israel

with Contributors

Alexander Remorov	Canada
Darij Grinberg	Germany
Harun Siljak	Bosnia and Herzegovina
Marin Misur	Croatia

Contents

Chapter 1

Problems

Problem 1.0.1 (PEN K11). *(Canada 2002) Find all functions $f : \mathbb{N}_0 \to \mathbb{N}_0$ such that for all $m, n \in \mathbb{N}_0$:*

$$mf(n) + nf(m) = (m+n)f(m^2+n^2). \tag{1.1}$$

Alexander Remorov (Canada)

Problem 1.0.2 (PEN I10). *Show that for all primes p,*

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \frac{(p+1)(p-1)(p-2)}{4}. \tag{1.2}$$

Cosmin Pohoata (Romania)

Problem 1.0.3 (PEN A14 A71). *A14 Let $n > 1$ be an integer. Show that n does not divide*

$$2^n - 1 \tag{1.3}$$

A71 Determine all integers $n > 1$ such that

$$\frac{2^n+1}{n^2} \tag{1.4}$$

is an integer.

Daniel Kohen (Argentina)

Problem 1.0.4 (PEN N17). *Suppose that a and b are distinct real numbers such that:*

$$a-b, a^2-b^2, \cdots, a^k-b^k, \cdots \tag{1.5}$$

are all integers. Show that a and b are integers.

Ofir Gorodetsky (Israel)

Problem 1.0.5 (PEN D5 D6)**.** *D5 Prove that for $n \geq 2$,*

$$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n \text{ terms}} \equiv \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n-1 \text{ terms}} \pmod{n}. \tag{1.6}$$

D6 Show that, for any fixed integer $n \geq 1$ the sequence

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \cdots \pmod{n} \tag{1.7}$$

is eventually constant.

Soo-Hong Lee (Korea), Harun Siljak (Bosnia and Herzegovina), Marin Misur (Croatia)

Problem 1.0.6 (PEN C2)**.** *The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?*

Ho Chung Siu (Hong Kong)

Problem 1.0.7 (PEN A13)**.** *Show that for all prime numbers p,*

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1}$$

is an integer.

Cosmin Pohoata (Romania)

Problem 1.0.8 (PEN A23, A24)**.** A23. *Prove that if $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ is expressed as a fraction, where $p > 3$ is a prime, then p^2 divides the numerator.*

A24. *Let $p > 3$ be a prime number and $k = \lfloor \frac{2p}{3} \rfloor$ Prove that $\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$ is divisible by p^2.*

Daniel Kohen (Argentina)

Problem 1.0.9 (PEN E16)**.** *Prove that for any prime p in the interval $\left]n, \dfrac{4n}{3}\right]$, p divides*

$$\sum_{j=0}^{n} \binom{n}{j}^4.$$

Darij Grinberg (Germany)

Problem 1.0.10 (PEN A37, A9, O51)**.** A37. *If n is a natural number, prove that the number $(n+1)(n+2)\cdots(n+10)$ is not a perfect square.*

A9. *Prove that among any ten consecutive positive integers at least one is relatively prime to the product of the others.*

O51. *Prove the among 16 consecutive integers it is always possible to find one which is relatively prime to all the rest.*

Harun Siljak (Bosnia and Herzegovina)

Chapter 2

Articles

2.1 Three Ways to Attack a Functional Equation

Alexander Remorov

1 (Canada 2002) Find all functions $f : \mathbb{N}_0 \to \mathbb{N}_0$ such that for all m, $n \in \mathbb{N}_0$:

PEN K11

$$mf(n) + nf(m) = (m+n)f(m^2+n^2). \tag{2.1}$$

First Solution. We claim that the only function satisfying the conditions is the constant function.

Assume there exists $a, b \in \mathbb{N} : f(a) > f(b)$. Take a, b such that $f(a) - f(b)$ is minimal. Then:

$$(a+b)f(b) < af(b) + bf(a) < (a+b)f(a) \tag{2.2}$$

From the given functional equation, $af(b) + bf(a) = (a+b)f(a^2+b^2)$. Substituting this into (1) gives:

$$(a+b)f(b) < (a+b)f(a^2+b^2) < (a+b)f(a) \Rightarrow f(b) < f(a^2+b^2) < f(a) \tag{2.3}$$

Then $f(a^2+b^2) - f(b) < f(a) - f(b)$, contradicting the choice of a and b. Hence the existence of $a, b \in \mathbb{N}$: $f(a) \neq f(b)$ is impossible. Hence there exists $t \in \mathbb{N}_0 : \forall x \in \mathbb{N} : f(x) = t$.

Finally, substituting $m = 0, n = 1$ into the original functional equation, we obtain that $f(0) = f(1)$. Hence there exists $t \in \mathbb{N}_0 : \forall x \in \mathbb{N}_0 : f(x) = t$. It is clear that that any $t \in \mathbb{N}_0$ woks. Therefore the only solution is $\forall x \in \mathbb{N}_0 : f(x) = t$ for any fixed $t \in \mathbb{N}_0$.

In the above solution, the key idea was using the extremal principle and arriving at a contradiction because of (2). This technique is applicable to this problem because of the discreteness of integers and is often used in solving many equations related to integers, including diophantine equations, where very often the first step is taking the minimal solution and then trying to find a smaller one. □

Second Solution. Let $f(0) = z$. Let S be the set of all non-negative integers such that $\forall x \in S$: $f(x) = z$. Clearly $0 \in S$. We note that:

1. Plugging into the functional equation $m = 0, n = t \in \mathbb{N}_0$, we get $tf(0) = tf(t^2) \Rightarrow f(t^2) = f(0)$, so:

$$\forall t \in \mathbb{N} : t^2 \in S \tag{2.4}$$

2. If $a, b \in S$, then substituting $m = a, n = b$ into the functional equation, we get $af(b) + bf(a) = (a + b)f(a^2 + b^2)$. But $a, b \in S$, so $f(b) = f(a) = z$, so we get:

$$(a + b)f(a^2 + b^2) = af(0) + bf(0) \Rightarrow f(a^2 + b^2) = z \tag{2.5}$$

Therefore:

$$\forall a, b \in S : a^2 + b^2 \in S \tag{2.6}$$

3. If $a, b, c, d \in \mathbb{N}, a, b, c \in S, a^2 + b^2 = c^2 + d^2$ then from (2), $a, b \in S \Rightarrow a^2 + b^2 \in S$. Also substituting $m = c, n = d$ into the functional equation, we get: $cf(d) + df(c) = (c + d)f(c^2 + d^2)$. But $c \in S, c^2 + d^2 = a^2 + b^2 \in S \Rightarrow f(c) = z, f(c^2 + d^2) = z$, so

$$cf(d) + dz = (c + d)z \Rightarrow f(d) = z \tag{2.7}$$

Hence:

$$\forall a, b, c, d \in \mathbb{N}, a, b, c \in S, a^2 + b^2 = c^2 + d^2 : d \in S. \tag{2.8}$$

Now we can use the properties (3), (5), (7) of the function to solve the problem. Let us first prove $x \in S$ for small positive integers x.

$1 = 1^2$,so by (3), we get $1 \in S$.
$2 = 1^2 + 1^2, 1 \in S$ so by (5), we get $2 \in S$.
$4 = 2^2$, so by (3), we get $4 \in S$.
Substituting $m = 3, n = 4$ into the functional equation we obtain $4f(3) + 3f(4) = 7f(25)$; $25 = 5^2 \in S, 4 \in S$, so $4f(3) + 3z = 7z \Rightarrow f(3) = z \Rightarrow 3 \in S$.
$5 = 2^2 + 1^2; 1, 2 \in S$, so by (5), we get $5 \in S$.
Therefore, $1, 2, 3, 4, 5 \in S$.

Let us now use mathematical induction on t to prove that

$$\forall t \in \mathbb{N}, t \geq 5 : 1, 2, 3, \ldots, t \in S \tag{2.9}$$

BASE STEP We have proved (8) for $t = 5$ in the previous paragraph.

INDUCTION STEP Assume (8) holds for $t = r - 1 \in \mathbb{N}, r \geq 5$. We need to prove (8) for $t = r$. We consider two cases:

Case 1 r is odd. Then we need to prove $r \in S$. It is quite natural to try to use (7) in order to prove $r \in S$. Let us look for integers $a, b, c \in S$, such that $a^2 + b^2 = c^2 + r^2$. Note $1, 2, \ldots, r-1 \in S$, so it is enough to find $a, b, c \in \{1, 2, \ldots, r-1\}$. Take $a = r-2$, then:

$$a^2 + b^2 = c^2 + r^2 \Leftrightarrow (r-2)^2 + b^2 = c^2 + r^2 \Leftrightarrow b^2 - c^2 = 4(r-1) \tag{2.10}$$

Now r is odd, so $r-1$ is even, so $r-1 = 2s$, hence we just need to find $b, c \in \{1, 2, \ldots, r-1\}$ so that $b^2 - c^2 = 8s$, and then $r \in S$ by (7).
If we set $b - c = 4, b + c = 2s$, we get $b = s + 2, c = s - 2$, and as $r - 1$ is even and is greater than or equal to 5, $r - 1 \geq 6 \Rightarrow 2s \geq 6 \Rightarrow s \geq 3$. But then $s + 2 < 2s \Leftrightarrow s > 2$, which is true for $s \geq 3$. Also $s \geq 3 \Rightarrow s - 2 \geq 1$. So $b = s+2, c = s-2 \in \{1, 2, \ldots, r-1\}$, hence $a = r-2, b = s+2, c = s-2 \in S$ and $a^2 + b^2 = c^2 + r^2$, so by (7), $r \in S$, so (8) holds for $t = r$ if r is odd.

Case 2 r is even. We will try to use the same technique as in case 1. However, this time taking $a = r - 2$ will not work, as we would then get $b^2 - c^2 = 4(r-1)$, but now $r - 1$ is odd and can be prime, and then we would not find the desired $b, c \in \{1, 2, \ldots, r-1\}$. But we can take $a = r - 4$, because then:

$$b^2 - c^2 = r^2 - (r-4)^2 = 8(r-2) = 16u \tag{2.11}$$

where $r - 2 = 2u$, as it is even, because r is even. Then we set $b - c = 8, b + c = 2u \Rightarrow b = u + 4, c = u - 4$. Then

$$b = u + 4 < 2u + 1 = r - 1 \Leftrightarrow u > 3, c = u - 4 \geq 1 \Leftrightarrow u \geq 5 \tag{2.12}$$

So if $u \geq 5$, the desired a, b, c exist, as then $a = r - 4, b = u + 4, c = u - 4 \in \{1, 2, \ldots, r-1\}$, $a^2 + b^2 = c^2 + r^2$, so by (7), $r \in S$ and (8) holds for $t = r$ if r is even and $2u = r - 2 \geq 10 \Leftrightarrow r \geq 12$. Hence it remains to prove the result for $r = 6, 8, 10$.

From case 1, we get that for x odd, $x \geq 5, x \in S$. Then $7 \in S, 9 \in S$. Now $4, 7, 9 \in S; 6^2 + 7^2 = 9^2 + 4^2$, so by (7), $6 \in S$. Also $8 = 2^2 + 2^2; 2 \in S \Rightarrow 8 \in S$ by (5). Finally $10 = 3^2 + 1^2; 1, 3 \in S \Rightarrow 10 \in S$ by (5).

By mathematical induction it follows that (8) holds for all $t \in \mathbb{N}$, and it immediately follows that the only solution is $\forall x \in \mathbb{N}_0 : f(x) = t$ for any fixed $t \in \mathbb{N}_0$.

Note that we did not use the original functional equation in the solution after establishing (3), (5) and (7). However, (3), (5) and (7) give us less freedom than the original functional equation, but these three relations allow to transform the problem of solving a functional equation into the problem of proving that the set of non-negative integers satisfying (3), (5), (7) is the set of all non-negative integers, and problems like this are very often solved using mathematical induction. □

Third Solution. A very standard technique for solving functional equations with a unique solution is to consider the function $g(x) = f(x) - h(x)$, where $f(x)$ is the original function, and $h(x)$ is the solution. This is useful because $g(x)$ must be 0 for all x in the domain, which often makes it easier to prove that $g(x)$ is always 0, especially when there are no expressions of the form $f(f(x)), f(f(f(x)))$, etc. In this problem, we can see that $f(x) = f(0)$ is a solution and probably is the only solution. So, let us consider $g(x) = f(x) - f(0)$.

Substituting $f(x) = g(x) + f(0)$ into the original functional equation, we get:

$$mg(n) + ng(m) = (m + n)g(m^2 + n^2) \tag{2.13}$$

Now, $g(0) = 0$. Substituting $m = 0, n = t \in \mathbb{N}$ into (12), we obtain $tg(0) = tg(t^2) \Rightarrow g(t^2) = g(0) = 0$. Therefore

$$\forall t \in \mathbb{N} : g(t^2) = 0 \tag{2.14}$$

Substituting into (12) $m = a, n = b, a, b \in \mathbb{N}, a > b$ such that there exists $c \in \mathbb{N} : a^2 + b^2 = c^2$, we get:

$$ag(b) + bg(a) = (a + b)g(a^2 + b^2) = (a + b)g(c^2) = 0 = g(a^2 + b^2) \tag{2.15}$$

Therefore:

$$g(a) = -\frac{a}{b}g(b), a > b \Rightarrow |g(a)| > |g(b)| \tag{2.16}$$

This is very powerful, as we notice that $g(x) = f(x) - f(0)$ is bounded from below, because $f : \mathbb{N}_0 \to \mathbb{N}_0$. Assume there exists $r \in \mathbb{N} : g(r) \neq 0$. Clearly $r \neq 0$. We just now need to construct an infinite sequence of positive integers $r = x_0 < x_1 < x_2 \ldots$ such that for $i = 1, 2, 3 \ldots$, there exist $y_i \in \mathbb{Z} : x_{i-1}^2 + x_i^2 = y_i^2$, because then from (15), $|g(x_0)| < |g(x_1)| < |g(x_2)| < \ldots$, and the signs of $g(x_i), g(x_{i+1})$ will be different. But $\forall x \in \mathbb{N} : f(x), f(0) \in \mathbb{N}_0 \Rightarrow g(x) \in \mathbb{Z}$. Then

$$|g(x_0)| < |g(x_1)| < |g(x_2)| < \ldots \Rightarrow |g(x_z)| \geq |g(x_{z-1})| + 1 \geq |g(x_{z-1})| + 2 \geq \ldots \geq |g(x_0)| + z \tag{2.17}$$

Then for z sufficiently large, $|g(x_z)| > f(0)$. But then $|g(x_{z+1})| > f(0)$, and one of $g(x_z), g(x_{z+1})$ is negative and is less than $-f(0)$, but this is impossible as $\forall x \in \mathbb{N} : g(x) = f(x) - f(0) \geq -f(0)$. Therefore the existence of $r \in \mathbb{N} : g(r) \neq 0$ is impossible, so $\forall x \in \mathbb{N}_0 : f(x) = f(0)$, and we would be done as long as we can construct the sequence $r = x_0 < x_1 < x_2 \ldots$

From the second solution, we proved that $f(1) = f(2) = f(3) = f(4) = f(0)$ so $g(1) = g(2) = g(3) = g(4) = 0$. Hence the $r \in \mathbb{N}$ for which $g(r) \neq 0$ must be greater than 4. Let us prove that $\forall k \in \mathbb{N}, k > 4$ we can find $l \in \mathbb{N}, l > k : \exists p \in \mathbb{N} : k^2 + l^2 = p^2$.

If k is even, let $k = 2h$, then we can take $l = h^2 - 1$, then $l^2 + k^2 = (k^2 + 1)^2$. Also $l > k$ as $h^2 - 1 > 2h \Leftrightarrow h^2 - 2h + 1 \geq 2 \Leftrightarrow (h - 1)^2 \geq 2$, which is true because $k = 2h > 4$. Hence if $x_i = 2g$ is an even term in the sequence $r = x_0 < x_1 < x_2 \ldots$, we set $x_{i+1} = g^2 + 1$, then x_{i+1} satisfies all of the properties of the sequence.

If k is odd, let $k = 2h + 1$, then it is more difficult to find l. It would be convenient for us to take l so that $l^2 + k^2 = Q(h)$ is a fourth degree polynomial in h, which is a perfect square for all h. We see that $k^2 = 4h^2 + 4h + 1$, then if $l = P(h)$ has a free term $q \in \mathbb{Z}$, then $Q(h)$ has a free term q^2+1, which must be a perfect square, so $q = 0$. Now as $Q(h)$ is a fourth degree polynomial, $P(h)$ is a second degree polynomial with free term of 0, so it has the form $wh^2 + vh$. In this case,

$$Q(h) = (w^2)h^4 + (2vw)h^3 + (v^2 + 4)h^2 + 4h + 1 = (R(h))^2 \tag{2.18}$$

for some polynomial $R(h)$ with integer coefficients. This polynomial is also second degree, and because in $Q(h)$ the leading coefficient is w^2 and the free coefficient is 1, $R(h) = wh^2 + sh + 1$ for some $s \in \mathbb{Z}$. But the coefficient in $Q(h)$ for h is 4, which is equal to the coefficient for h in $(R(h))^2$, which is $2s$, hence $s = 2$. Then the coefficient for h^3 in $(R(h))^2$ is $4w$, which must be equal to the coefficient for h^3 in $Q(h)$, which is $2vw$, hence we have $v = 2$.

Also the coefficient for h^2 in $(R(h))^2$ is $2w+4$, which must be equal to the coefficient for h^2 in $Q(h)$, which is v^2+4, hence we have $2w = v^2 = 2^2 \Rightarrow w = 2$. So $v = w = 2$, so $l = 2h^2+2h$. It is easy to check that $l^2 + k^2 = (2h^2 + 2h)^2 + (2h + 1)^2 = (2h^2 + 2h + 1)^2$, and so $l = 2h^2 + 2h > 2h + 1 = k$. Hence if $x_i = 2g + 1$ is an odd term in the sequence $r = x_0 < x_1 < x_2 \ldots$, we set $x_{i+1} = 2g^2 + 2g$, then x_{i+1} satisfies all of the properties of the sequence.

Therefore, starting with r, we can always construct the next term in the sequence depending on the parity of the current term, and as a result, the required infinite sequence $r = x_0 < x_1 < x_2 \ldots$ exists, from where it follows that $\forall x \in \mathbb{N} : g(x) = 0$, so the only solution is $\forall x \in \mathbb{N}_0 : f(x) = t$ for any fixed $t \in \mathbb{N}_0$. □

References

1 *Canadian Mathematical Olympiad 2002 Solutions*, http://www.math.ca/Competitions/CMO/

2 *PEN Problem K11*, http://www.artofproblemsolving.com/Forum/viewtopic.php?t=150754

2.2 A Generalization of an Identity

Cosmin Pohoata

2 Show that for all primes p,

PEN I10

$$\sum_{k=1}^{p-1}\left\lfloor\frac{k^3}{p}\right\rfloor=\frac{(p+1)(p-1)(p-2)}{4}.$$

First Solution. For $1 \le k \le p-1$, we have $k^3 \not\equiv 0 \mod p$ and $(p-k)^3 \equiv -(k^3) \mod p$, and therefore

$$\left(\frac{k^3}{p}-\left\lfloor\frac{k^3}{p}\right\rfloor\right)+\left(\frac{(p-k)^3}{p}-\left\lfloor\frac{(p-k)^3}{p}\right\rfloor\right)=1.$$

Hence,

$$\begin{aligned}\sum_{k=1}^{p-1}\left\lfloor\frac{k^3}{p}\right\rfloor &= \sum_{k=1}^{p-1}\frac{k^3}{p}-\sum_{k=1}^{p-1}\left(\frac{k^3}{p}-\left\lfloor\frac{k^3}{p}\right\rfloor\right)\\ &= \frac{1}{p}\left(\sum_{k=1}^{p-1}k^3\right)-\frac{1}{2}\sum_{k=1}^{p-1}\left[\left(\frac{k^3}{p}-\left\lfloor\frac{k^3}{p}\right\rfloor\right)+\left(\frac{(p-k)^3}{p}-\left\lfloor\frac{(p-k)^3}{p}\right\rfloor\right)\right]\\ &= \frac{1}{p}\left(\frac{p(p-1)}{2}\right)^2-\frac{p-1}{2}\\ &= \frac{(p-2)(p-1)(p+1)}{4}.\end{aligned}$$

□

Second Solution. Motivated by this solution, we show a natural generalization:

Proposition 2.2.1. *Let p be an odd prime and let q be an integer that is not divisible by p. If $f : \mathbb{Z}_+^* \to \mathbb{R}$ is a function such that:*

i) $\frac{f(k)}{p}$ is not an integer, for any $k = 1, 2, \ldots, p-1$;

ii) $f(k) + f(p-k)$ is an integer divisible by p, for any $k = 1, 2, \ldots, p-1$,

then

$$\sum_{k=1}^{p-1}\left\lfloor\frac{qf(k)}{p}\right\rfloor=\frac{q}{p}\cdot\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}.$$

Proof. From *ii*) it follows that

$$\frac{qf(k)}{p}+\frac{qf(p-k)}{p}\in\mathbb{Z}.$$

From *i*) we obtain that $\frac{qf(k)}{p}\notin\mathbb{Z}$ and $\frac{qf(p-k)}{p}\notin\mathbb{Z}$, for any $k = 1, 2, \ldots, p-1$, and hence

$$0<\left\{\frac{qf(k)}{p}\right\}+\left\{\frac{qf(p-k)}{p}\right\}<2.$$

On other hand,

$$\left\{\frac{qf(k)}{p}\right\}+\left\{\frac{qf(p-k)}{p}\right\}=\left(\frac{qf(k)}{p}+\frac{qf(p-k)}{p}\right)-\left(\left\lfloor\frac{qf(k)}{p}\right\rfloor+\left\lfloor\frac{qf(k)}{p}\right\rfloor\right),$$

and thus, because $\frac{qf(k)}{p} + \frac{qf(p-k)}{p} \in \mathbb{Z}$, we deduce that

$$\left\{\frac{qf(k)}{p}\right\} + \left\{\frac{qf(p-k)}{p}\right\} \in \mathbb{Z}.$$

It now follows that

$$\left\{\frac{qf(k)}{p}\right\} + \left\{\frac{qf(p-k)}{p}\right\} = 1, \quad \text{for any } k = 1,\ 2,\ \ldots,\ p-1.$$

Summing up and dividing by 2 yields

$$\sum_{k=1}^{p-1} \left\{\frac{qf(k)}{p}\right\} = \frac{p-1}{2},$$

and therefore,

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

This proves Proposition 1. □

Obviously, the function $f(x) = x^3$ satisfies both conditions from Proposition 2.2.1. Hence,

$$\begin{aligned}\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor &= \frac{q}{p} \cdot \sum_{k=1}^{p-1} k^3 - \frac{p-1}{2}\\ &= \frac{q}{p} \cdot \left(\frac{(p-1)p}{2}\right)^2 - \frac{p-1}{2}\\ &= \frac{(p-2)(p-1)(p+1)}{4}.\end{aligned}$$

We now proceed with another two applications of Proposition 2.2.1. We begin with Gauss' celebrated formula.

Proposition 2.2.2. *(Gauss) Let p and q be two relatively prime integers. The following identity holds:*

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

Proof. The function $f(x) = x$ satisfies both conditions in Proposition 2.2.1. Hence,

$$\begin{aligned}\sum_{k=1}^{p-1} \left\lfloor \frac{qk}{p} \right\rfloor &= \frac{q}{p} \cdot \sum_{k=1}^{p-1} k - \frac{p-1}{2}\\ &= \frac{q}{p} \cdot \frac{(p-1)p}{2} - \frac{p-1}{2}\\ &= \frac{(p-1)(q-1)}{2}.\end{aligned}$$

□

Proposition 2.2.3. *(MathLinks, some olympiad - to add source) Let p be an odd prime. Show that*

$$\sum_{k=1}^{p-1} \frac{k^p - k}{p} \equiv \frac{p+1}{2} \pmod{p}.$$

Proof. The function $f(x) = \frac{x^p}{p}$ satisfies both conditions in Proposition 2.2.1. Thus, by setting $q = 1$ (note that we are allowed to do that), we get

$$\begin{aligned}\sum_{k=1}^{p-1} \left\lfloor \frac{k^p}{p^2} \right\rfloor &= \frac{1}{p} \cdot \sum_{k=1}^{p-1} \frac{k^p}{p} - \frac{p-1}{2} \\ &= \frac{1}{p} \cdot \sum_{k=1}^{p-1} \frac{k^p}{p} - \frac{1}{p^2} \cdot \sum_{k=1}^{p-1} k + \frac{1}{p^2} \cdot \frac{(p-1)p}{2} - \frac{p-1}{2} \\ &= \frac{1}{p} \cdot \sum_{k=1}^{p-1} \frac{k^p - k}{p} - \frac{1}{p} \cdot \frac{(p-1)^2}{2}.\end{aligned}$$

Thus,

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

and therefore

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{k^p - k}{p} &\equiv \frac{(p-1)^2}{2} \pmod{p} \\ &\equiv \frac{p^2+1}{2} \pmod{p} \\ &\equiv \frac{p+1}{2} \pmod{p}.\end{aligned}$$

□

□

2.3 Minimum prime divisors

Daniel Kohen

3 A14 Let $n > 1$ be an integer. Show that n does not divide

PEN A14
A71

$$2^n - 1 \tag{2.19}$$

A71 Determine all integers $n > 1$ such that

$$\frac{2^n + 1}{n^2} \tag{2.20}$$

is an integer.

Proof. First we will introduce some definitions and we will provide the proof of an elementary fact. Let d be the least natural number that satisfies

$$a^d \equiv 1 \pmod p \tag{2.21}$$

Then we write

$$ord_p a = d \tag{2.22}$$

Lemma 1:

$$a^k \equiv 1 \pmod p \iff k \equiv 0 \pmod{ord_p a} \tag{2.23}$$

Proof:

$$ord_p a = d \tag{2.24}$$

Let $k = dt + r$, $d > r \geq 0$ (which is valid by the division algorithm)

So we get that

$$a^{dt+r} \equiv 1 \pmod p \tag{2.25}$$

Since $a^d \equiv 1 \pmod p \Longrightarrow a^{dt} \equiv 1 \pmod p \Longrightarrow a^r \equiv 1 \pmod p$ but

$$d > r \tag{2.26}$$

If $r = 0$ the claims follows and if $r > 0$ we are contradicting the minimality of d, so we see that this is not possible.

It is worthy to stop here and analyze the importance of the definition we have just introduced. It not only uses elementary number theory but also relies on a very powerful principle that states that every set of natural numbers has an element which is less than the others.Clearly the idea of a least-element allows us to find contradictions about minimality after supposing a number satisfies a given condition and is the smallest of the sort. This is a key concept in maths; especially in number theory.

Now we are ready to begin our proof of A14

Since $n > 1$, n has a prime divisor, then we can choose it so that it is minimal. Clearly if n is even we get that $2^n - 1$ is odd. An even number can't divide an odd number so n is odd. Let p be the minimal prime that divides n $(p > 2)$ We can write $n = pk$

$$2^{pk} \equiv 1 \pmod{p} \tag{2.27}$$

Because $2^p \equiv 2 \pmod{p}$ by Fermat's little theorem, we get that

$$2^k \equiv 1 \pmod{p} \tag{2.28}$$

Let

$$d = ord_p 2 \tag{2.29}$$

So $k = dt$ for some integer t

Clearly $d > 1$

Since $2^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem , we obtain

$$p - 1 \equiv 0 \pmod{d} \tag{2.30}$$

so

$$1 < d \leq p - 1 < p \tag{2.31}$$

We obtain that d is a divisor of k,and it follows it is also a divisor of n. Because $p > d > 1$, we are contradicting the minimality of p; it follows that this is not possible, so there are not any solutions for $n > 1$, as we wished to prove.

A71 Proof: Clearly n is odd.Again we define p as the least prime divisor of n. We have that

$$2^n \equiv -1 \pmod{p} \tag{2.32}$$

squaring both sides

$$2^{2n} \equiv 1 \pmod{p} \tag{2.33}$$

Again we put $n = pk$ and we have, reasoning in the same way as the previous problem, that

$$2^{2k} \equiv 1 \pmod{p} \tag{2.34}$$

Let

$$d = ord_p 2 \tag{2.35}$$

Then $2k \equiv 0 \pmod{d}$ and $p - 1 \equiv 0 \pmod{d}$ If $gcd(k, d) > 1$, as exposed before, $gcd(d, n) > 1$ and d is smaller than p, which is absurd. So the only possibility is that d divides 2.

$d = 1$ is not possible

$d = 2$ we have that

$$2^2 \equiv 1 \pmod{p} \Longrightarrow p = 3 \tag{2.36}$$

Hensel Lemma (Lifting the exponent): Let p be an odd prime. Suppose that $a \equiv b \pmod{p}$ $(gcd(ab, p) = 1)$ Let's define X as the maximum exponent of p dividing $a - b$ and Y the maximum exponent of p dividing the positive number m. Then

$$X + Y \tag{2.37}$$

is the maximum exponent of p dividing

$$a^m - b^m \tag{2.38}$$

Now,back to the problem, let X be the exponent of 3 in n Since n^2 divides $2^{2n} - 1$ Then we get: $2X$ is the exponent of 3 in n^2 Since the exponent of 3 in $2^2 - 1$ is 1 we have that the exponent of 3 in $2^{2n} - 1$ is $X + 1$ So we must have

$$X + 1 \geq 2X \implies X = 1 \tag{2.39}$$

Then we may write $n = 3t$ with $gcd(3, t) = 1$

Now we will continue with our reasoning, as shown before. Let q be the least prime divisor of t

$$t = ql \tag{2.40}$$

Again we get that

$$2^{6l} \equiv 1 \pmod{q} \tag{2.41}$$

Then if

$$c = ord_q 2 \tag{2.42}$$

easily we conclude that c divides $6l$ and if $gcd(l, c) > 1$ we will get a similar contradiction as in previous lines. So c divides 6 the cases $c = 1$ and $c = 2$ lead to $q = 1$ implying $n = 3$ which works and $q = 3$ which doesn't make any sense

If $c = 3$ or $c = 6$ replacing in

$$2^c \equiv 1 \pmod{q} \implies q = 7 \tag{2.43}$$

We must have

$$2^n \equiv -1 \pmod{7} \tag{2.44}$$

It is easy to check that $2^1 \equiv 2 \pmod{7}$ $2^2 \equiv 4 \pmod{7}$ $2^3 \equiv 1 \pmod{7}$ But $2^{k+3} \equiv 2^3 2^k \equiv 2^k$ $\pmod{7}$ So for all k , $2^k \not\equiv -1 \pmod{7}$ As a corollary the only posibility is that $n = 3$ which indeed satisfies the equation. The proof is finished.

□

References

1 *PEN Problem A14*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150382.

2 *PEN Problem A71*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150439

2.4 Different Approaches to an Intuitive Problem

Ofir Gorodetsky

4
PEN N17

Suppose that a and b are distinct real numbers such that:

$$a-b, a^2-b^2, \cdots, a^k-b^k, \cdots \tag{2.45}$$

are all integers. Show that a and b are integers.

First Solution. Let $x_n = a^n - b^n$. We are given that $x_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$. We can easily deduce that a, b are rational: $\frac{\frac{x_2}{x_1} \pm x_1}{2} = \frac{a+b\pm(a-b)}{2} = a, b$.
Assume, for contradiction's sake, that a is not an integer. We'll have $a = \frac{p}{q}$, $(p,q) = 1$, and $|q| > 1$. There exist $m \in \mathbb{N}_0$ such that $q^m \mid a-b, q^{m+1} \nmid a-b$. We have $\left(x_1 + \frac{p}{q}\right)^n - \left(\frac{p}{q}\right)^n = x_n$, or equivalently:

$$\left(x' q^{m+1} + p\right)^n - p^n = q^n x_n \tag{2.46}$$

For a suitable integer x'. Now we'll use the binomial theorem and divide by q^{m+1}:

$$\sum_{i=0}^{n-1} \binom{n}{i} p^i x'^{n-i} q^{(m+1)(n-i-1)} = q^{n-m-1} x_n. \tag{2.47}$$

Looking $\pmod q$, for $n > m+1$, we see that: $x' p^{n-1} n \equiv 0 \pmod q$. Exploiting the fact that $(q,p) = 1$ and taking $n = (m+2)|q| + 1$, yields $q|x'$, a contradiction. Hence, $q = \pm 1$ and a is an integer. $b = a - x_1$ is thus also an integer, Q.E.D.

□

Remark: notice the similarities to the proof of the Rational root theorem.

Second Solution. Notice the following identity:

$$x_{n+1}^2 - x_n x_{n+2} = (ab)^n x_1^2 \tag{2.48}$$

It can be proved directly for every natural n:
$x_n x_{n+2} - x_{n+1}^2 = (a^n - b^n)\left(a^{n+2} - b^{n+2}\right) - \left(a^{n+1} - b^{n+1}\right)^2 = a^{2n+2} - b^2 (ab)^n - a^2 (ab)^n + b^{2n+2} - a^{2n+2} + 2(ab)^{n+1} - b^{2n+2} = -(ab)^n (a-b)^2 = -(ab)^n x_1^2$.
The motivation for it is the known identity $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$ satisfied by the Fibonacci sequence: $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{N}_0$. x_n is a linear recurrence sequence, with its first term being 0 (if we consider x_0), like F_n. From its form we deduce that the roots of its characteristic equation are a and b. Thus, given that $a \neq b$, the equation is $x^2 - (a+b)x + ab = 0$, hence x_n follows that recursion $x_{n+2} = (a+b)x_{n+1} - ab x_n$.

Assume to the contrary that ab is not an integer. It can be represented in the form $\frac{p}{q}$, where p, q are relatively prime integers and $|q| > 1$. From (2.22), we have: $q^n | x_1^2 p^n$ For all n (because the expression on the left is an integer). From the fact that $(p,q) = 1$ it follows that $q^n | x_1^2$. x_1 is non-zero, hence $x_1^2 \geq q^n \geq 2^n$. This is true for all $n \in \mathbb{N}$ and it's a contradiction. Hence $|q| = 1$

and ab is an integer. $a-b=x_1$ is an integer also. Let $a=\frac{p_1}{q}, b=\frac{p_2}{q}$ $(p_{1,2}, q \in \mathbb{Z})$. We know that $q^2 | p_1 p_2, q | p_1 - p_2$. We'll manipulate it as follows:

$$q^2 \mid (p_1-p_2)^2 + 4p_1p_2 = (p_1+p_2)^2 \implies q \mid p_1 \pm p_2 \implies q \mid 2p_{1,2} \tag{2.49}$$

We have 2 options: either a and b are both integers, or are half-integers, i.e. take the form $k_{1,2}+0.5$ for some integers $k_{1,2}$. We can see that the 2nd option is not valid in two different ways:
1. $a^n - b^n \in \mathbb{Z}$ is equivalent to $2^n \mid (2k_1+1)^n - (2k_2+1)^n$. For $n = 2^l$ We can factor it as follows:

$$(2k_1+1)^{2^l} - (2k_2+1)^{2^l} = 2(k_1-k_2)\prod_{i=0}^{l-1}\left((2k_1+1)^{2^i} + (2k_2+1)^{2^i}\right) \tag{2.50}$$

An expression of the form $a^{2^i} + b^{2^i}$, where a, b are odd and i is positive, is never divisible by 4. This is a direct consequence of $t^2 \equiv 1 \pmod 4$ for $t \equiv 1 \pmod 2$ (choose $t = a^{2^{i-1}}, b^{2^{i-1}}$). Hence:

$$ord_2\left((2k_1+1)^{2^l} - (2k_2+1)^{2^l}\right) = l + ord_2\left((k_1-k_2)\left((2k_1+1)^2 + (2k_2+1)^2\right)\right) \tag{2.51}$$

For all $l \in \mathbb{N}$. This fact contradicts $ord_2\left((2k_1+1)^n - (2k_2+1)^n\right) \geq n$ for all $n \in \mathbb{N}$: just take $n = 2^l$ large enough.
2. We get that $ab = k_1k_2 + \frac{2k_1+2k_2+1}{4}$ is an integer, which is impossible (shorter, huh?). □

Third Solution. We'll prove 3 lemmas.
Lemma 1: For any odd prime p, and distinct a, b satisfying $a - b \equiv 0 \pmod p, (ab, p) = 1$, one has $ord_p(a^n - b^n) = ord_p(n) + ord_p(a-b)$.
Proof: it is equivalent to the identity

$$\left(a + bp^k\right)^{p^s t} - a^{p^s t} \equiv a^{p^s t - 1} btp^{s+k} \pmod{p^{s+k+1}} \tag{2.52}$$

for $k > 0$. It can be proved either by induction on $s \geq 0$, or by direct expanding:

$$\left(a + bp^k\right)^{p^s t} - a^{p^s t} = a^{p^s t-1} btp^{s+t} + \sum_{i=2}^{p^s t} \binom{p^s t}{i} a^{p^s t - i} p^{ki} b^i \tag{2.53}$$

It is enough to show that $ord_p\left(p^{ki}\binom{p^s t}{i}\right) \geq k + s$ for $i > 1$. Notice the following identity:

$$i\binom{p^s t}{i} = p^s t \binom{p^s t - 1}{i-1} \tag{2.54}$$

which implies: $ord_p\left(p^{ki}\binom{p^s t}{i}\right) \geq ki + s - ord_p i$.
If we put $i = p^j l > 1, (p, l) = 1$, we get: $ki + s - ord_p i = kp^j l + s - j \geq k3^j l + s - j$. What we want to show is: $k\left(3^j l - 1\right) \geq j + 1$. We have $k \geq 1$ as a condition.
For $j = 0$: $k\left(3^j l - 1\right) \geq 3^j l - 1 = l - 1 \geq 1 = j + 1$, because $i = l > 1$.
If $j > 0$: $k\left(3^j l - 1\right) \geq 3^j - 1 \geq j + 1$ (follows from $3^j \geq j + 2$ for $j \in \mathbb{N}$ - straightforward induction).
The result follows.
Lemma 2: For any distinct odd integers a, b we have $ord_2(a^n - b^n) = ord_2\left(\frac{a^2-b^2}{2}\right) + ord_2(n)$ for even $n \in \mathbb{N}$, and $ord_2(a^n - b^n) = ord_2(a-b)$ for odd $n \in \mathbb{N}$.
Proof: Both results follow directly from our work in the previous solution, and from the congruence

$\frac{a^n-b^n}{a-b} = \sum_{i=0}^{n-1} a^i b^{n-i-1} \equiv n \equiv 1 \pmod 2$ for odd n.

Lemma 3: For any positive number x, any real number y, and any prime p, the inequality $ord_p(n) \geq xn + y$ holds only for finitely many $n's$.

Proof: First step - let l be a non-negative integer. There are finitely many values of n that satisfy the inequality when $p^l || n$, namely: $n \leq \frac{l-y}{x}$. Second step - $p^l \geq l^{1.5}$ (induction). Third and last step - there are finitely many values of l that satisfy the inequality when $p^l || n$: $ord_p(n) \geq xn + y \implies l \geq xl^{1.5} + y$, or: $1 \geq x\sqrt{l} + \frac{y}{l}$. When l tends to infinity, the last expression tends to ∞, which yields the result.

Combining the 3 steps, we get the result stated by the lemma.

Now, as before, we let $a = \frac{x}{z}, b = \frac{y}{z}$ $(x \neq y)$. x_n is an integer for all $n \in \mathbb{N}$ is equivalent to:

$$\forall n \in \mathbb{N}, z^n \mid x^n - y^n \tag{2.55}$$

We'll prove that $z \mid (x, y)$, and it will solve the problem. Set $g = (x, y), x' = \frac{x}{g}, y' = \frac{y}{g}$.

Let p be an odd prime dividing z and set $k = ord_p(z)$. $x - y$ is divisible by z and hence by p. Also, denote o_p as the order of $x'y'^{-1}$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ (in the case when $(x', p) = (y', p) = 1$), i.e. the minimal number such that $p | x'^{o_p} - y'^{o_p}$.

If $o_p \nmid n$, or one of x', y' is divisible by p: because $ord_p(z)$ reduces multiplication to addition,

$$ord_p(x^n - y^n) = ord_p(x'^n - y'^n) + ord_p(g^n) = n\ ord_p(g) \tag{2.56}$$

If $o_p \mid n$: from the first lemma -

$$\begin{aligned} ord_p(x^n - y^n) & \\ &= ord_p(x'^n - y'^n) + ord_p(g^n) \\ &= ord_p(x'^{o_p} - y'^{o_p}) + ord_p\left(\frac{n}{o_p}\right) + n\ ord_p(g) \\ &= C + ord_p(n) + n\ ord_p(g) \end{aligned}$$

Combining those, we get the inequality: $nk = ord_p(z^n) \leq ord_p(x^n - y^n) \leq n\ ord_p(g) + |C| + ord_p(n)$, where C is suitable constant. By the 3rd lemma, it is possible for all n only if $ord_p(g) \geq k$.

The treatment of $p = 2$ is exactly the same using the 2nd lemma, except for the value of C, and we get $ord_2(x^n - y^n) \leq n\ ord_2(g) + ord_p(n) + |C|$ for a suitable constant C. By the 3rd lemma, it is possible only if $ord_2(g) \geq k$.

The result follows. □

Generalizations:

Proposition 2.4.1. *Suppose that a and b are distinct real numbers such that: $a^n - b^n \in \mathbb{Z}$ for any $n \in \mathbb{N}$ divisible by s or t, where s, t are relatively prime positive integers. Then a, b are integers.*

Proof. It follows from the original problem: apply our result, once with $a = a'^s, b = b'^s$ and once with $a = a'^t, b = b'^t$. We get that a^s, b^s, a^t, b^t are integers. In the case where both a and b are non-zero, by Bzout's lemma there are integers $k_{1,2}$ such that $sk_1 + tk_2 = 1$. We get: $a = (a^s)^{k_1} (a^t)^{k_2} \implies a \in \mathbb{Q}$. Together with $a^s \in \mathbb{Z}$ we get that $a \in \mathbb{Z}$. In the same way, $b \in \mathbb{Z}$. If

$a = b = 0$, we're done. If exactly one of $a = 0$, $b = 0$ is true, WLOG $a = 0$, as before we conclude that $b^s, b^t \in \mathbb{Z}$, and then $b \in \mathbb{Z}$. □

Proposition 2.4.2. *Suppose that a and b are distinct rational numbers such that: $a^n - b^n \in \mathbb{Z}$ for infinitely many $n \in \mathbb{N}$. Then a, b are integers.*

Proof. We could actually show this already in the third solution. We again reformulate the problem as follows - $z^n \mid x^n - y^n$ for infinitely many n's implies $z \mid (x, y)$ (when $x \neq y$). As before, we use the 3rd lemma and get $ord_p\left((x, y)\right) \geq ord_p z$, for all primes p dividing z, and the result follows. □

References and Further Reading

1 *PEN Problem N17*, http://www.mathlinks.ro/viewtopic.php?t=150843.

2 *A nice and tricky lemma (lifting the exponent) by Santiago Cuellar and Jose Alejandro Samper*, http://reflections.awesomemath.org/2007_3/Lifting_the_exponent.pdf.

2.5 Exponential Congruence Sequence

Soo-Hong Lee, Harun Siljak, Marin Misur

5 PEN M16 D5 D6

M16 Define a sequence a_n by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

D5 Prove that for $n \geq 2$,

$$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n \text{ terms}} \equiv \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n-1 \text{ terms}} \pmod{n}. \tag{2.57}$$

D6 Show that, for any fixed integer $n \geq 1$ the sequence

$$2,\ 2^2,\ 2^{2^2},\ 2^{2^{2^2}}, \cdots \pmod{n} \tag{2.58}$$

is eventually constant.

The first solution of problem M16 we'll present here is in a traditionalized, brute-force manner (which is rather straightforward):

Solution 1 (M16). First, we note that $a_1 \equiv 3 \pmod{100}$ and $a_2 \equiv 27 \pmod{100}$. Using square-and-multiply algorithm, we get:

$$\begin{aligned} 3^6 &\equiv 27^2 \equiv 29 \pmod{100}, \\ 3^{12} &\equiv 29^2 \equiv 41 \pmod{100}, \\ 3^{24} &\equiv 41^2 \equiv 81 \pmod{100}, \\ 3^{27} &\equiv 27 \times 81 \equiv 87 \pmod{100}. \end{aligned}$$

So, we have $a_3 \equiv 87 \pmod{100}$. What about a_4?
$3^{81} \equiv 87^3 \equiv 3 \pmod{100}$, $3^{87} \equiv 29 \times 3 \equiv 87 \pmod{100}$. So $a_4 \equiv 3^{100k}87 \pmod{100}$. This takes us to an interesting hypothesis: if $3^{100} \equiv 1 \pmod{100}$, then for every next m, $m \geq 3$, $a_m \equiv 87 \pmod{100}$. It follows that the answer to the question in the problem would be 87. Why?
$a_m = 100k + 87$, $a_{m+1} = 3^{100k+87} = 3^{100k}3^{87}$ and if the assumption about 3^{100} is true, it is congruent to $3^{87} \equiv 87 \pmod{100}$ and so on for next m.
$3^{100} = 3^1 \times 3^{12} \times 3^{87} \equiv 3 \times 41 \times 87 \equiv 1 \pmod{100}$, so the assumption is proven: 87 is the desired number. □

Logical question arises now: can the calculation be simplified in any manner? As we shall see, introducing few basic concepts will reduce the calculation to smaller numbers-such calculation would be far more worthwhile than the one we introduced: what if the desired residue appeared in tenth, and not in third iteration as in our case? The calculations would have been tedious and the following algorithm will make it fairly easy (also note that the first solution, unlike second, cannot be considered algorithmized, as algorithms exclude intuition and 'experimenting').

Solution 2 (M16). First, we'll introduce (without a proof) a very well known fact in number theory:

Proposition 2.5.1 (Euler's Theorem)**.** *If a and n are relatively prime, then*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{2.59}$$

where $\phi(n)$ is Euler's function: number of positive integers smaller than n which are relatively prime to n (which can be calculated as $\phi(n) = \prod_{i=1}^{k} \phi({p_i}^{c_i}) = \prod_{i=1}^{k} {p_i}^{c_i-1}(p_i - 1)$ if $n = \prod_{i=1}^{k} {p_i}^{c_i}$ represents the prime factorization of n).

Now, note that $a_i \equiv 3^{a_{i-1}} \equiv 3^{\text{ mod } (a_{i-1},\phi(100))} \pmod{100}$, so this congruence is determined by a_{i-1} taken $\pmod{\phi(100) = 40}$. Analoguously, the latter congruence is determined by a_{i-2} taken $\pmod{\phi(40) = 16}$. Now, next one is a_{i-3} taken $\pmod{\phi(16) = 8}$, determined by a_{i-4} $\pmod{\phi(8) = 4}$ and finally a_{i-5} $\pmod{\phi(4) = 2}$. Now, noting that $3 \equiv 1 \pmod{2}$

$$\begin{aligned}
a_{i-4} &\equiv 3^{a_{i-5}} \equiv 3^1 \equiv 3 \pmod{4},\\
a_{i-3} &\equiv 3^{a_{i-4}} \equiv 3^3 \equiv 3 \pmod{8},\\
a_{i-2} &\equiv 3^{a_{i-3}} \equiv 3^3 \equiv 11 \pmod{16},\\
a_{i-1} &\equiv 3^{a_{i-2}} \equiv 3^{11} \equiv 27 \pmod{40},\\
a_i &\equiv 3^{a_{i-1}} \equiv 3^{27} \equiv 87 \pmod{100},
\end{aligned}$$

□

Euler function in general case doesn't represent least value we're looking for. Using its reduced form (so-called Carmichael function), we can offer even shorter solution:

Solution 3 (M16).

Definition 2.5.1 (Carmichael function)**.** *If a and n are relatively prime, then Carmichael function $\lambda(n)$ represents the least positive integer for which*

$$a^{\lambda(n)} \equiv 1 \pmod{n} \tag{2.60}$$

holds. It can be calculated as $\lambda(n) = \operatorname{lcm}(\lambda({p_1}^{c_1}), \ldots, \lambda({p_n}^{c_n}))$ where

$$\lambda(p^c) = \begin{cases} \phi(p^c) = p^{c-1}(p-1) & \text{if } p > 2 \text{ or } p = 2, c < 3 \\ p^{c-2} & \text{if } p = 2, c \geq 3 \end{cases}$$

if $n = \prod_{i=1}^{k} {p_i}^{c_i}$ represents the prime factorization of n.

Now, using this fact, our iteration procedure from Solution 2 reduces to the chain 100 → 20 → 4 → 2, and as $a_{i-3} \equiv 1 \pmod{2}$:

$$\begin{aligned}
a_{i-2} &\equiv 3^{a_{i-3}} \equiv 3^1 \equiv 3 \pmod{4},\\
a_{i-1} &\equiv 3^{a_{i-2}} \equiv 3^3 \equiv 27 \pmod{20},\\
a_i &\equiv 3^{a_{i-1}} \equiv 3^7 \equiv 87 \pmod{100},
\end{aligned}$$

with the same conclusion as in Solution 2. □

It is quite natural to ask: is this sequence of threes 'special'? Can the numbers $3, 100$ be replaced with other integer constants? The answer to the latter question is yes, i.e. the following generalization holds:

Proposition 2.5.2 (Generalization)**.** *For arbitrary integers k, m, sequence defined by $a_1 = k, a_n = k^{a_{n-1}}$ becomes eventually constant $\pmod{m}$.*

Proof 1. Let's suppose the opposite, i.e. the Proposition is wrong for some positive integer m. Then there is a least such number (denote it with c). Obviously, $c \neq 1$. For all integers c, the sequence $a_n \pmod{c}$ eventually becomes cyclic (reader may try to prove this claim). We will denote the period of this cycle with t. The definition of t implies that there are $t-1$ nonzero residues modulo c, so $t \leq c-1 < c$. Since $(a_n)_{n=1}^{\infty}$ does not become constant $\pmod{c}$, it follows the sequence of exponents of these terms, i.e., the sequence (b_n), defined as $b_1 = 1, b_n = k^{b_{n-1}}$ does not become constant $\pmod{t}$. Then the problem statement is false for $m = t$. Since $t < c$, this yields a contradiction. Therefore the Proposition is true. □

Proof 2-outline. It is enough to prove the claim for $m = p^c$ where p is prime (and c is a positive integer). Why? By Chinese Remainder Theorem, if the Proposition holds for relatively prime modulii p and q, then it also holds for modulo pq (proof is straightforward). Now, if p divides c, the proof is trivial. If p isn't a divisor of c, then we can do the do the proof using strong induction on m, using Euler's Theorem. This technique will be efficiently used in the Solution (D5), so we will not go into details in this outline.

□

Notice that this generalization yields also the proof for D6 (in fact, this is generalized D6).

We have shown that these sequeces do converge, and what do they converge to in one particular case (M16). Now we will see when do they become constant, in case $a_1 = 2$ (D5).

Solution (D5). We can prove stronger statement by induction over n. First, write $a_n = \underbrace{2^{2^{\cdot^{\cdot^{2}}}}}_{n\text{times}}$

Proposition 2.5.3. $a_m \pmod{n}$ *is constant for all $m \geq n-1$.*

Proof. Base case $n = 1$ is obvious.
If n is even, write $n = 2^s t$. Then the sequence is clearly constant after $n-1$ modulo 2^s. It is also true for modulo t by the induction hypothesis.
So we can suppose that n is odd. Then there is a constant c satisfying

$$a_m \equiv c \pmod{\phi(n)} \tag{2.61}$$

for all m after $\phi(n) - 1 (\leq n-2)$. Thus $a_m \equiv 2^c \pmod{n} (m \leq n-1)$ by Euler Theorem, as desired. □

This can prove a following corollary.

Corollary 2.5.1. $\underbrace{2^{2^{\cdots^{2}}}}_{n\ terms} - \underbrace{2^{2^{\cdots^{2}}}}_{n-1\ terms}$ *is divisible by all positive integer less or equal than n.*

□

The form $2^{a_n} = a_{n+1}$ looks like ISL2006 N9. This can also lead to a little bit different problem.

Proposition 2.5.4. *Prove that for arbitrary positive integer n, there exists an integer m such that*

$$\frac{2^m - m}{n} \tag{2.62}$$

is integer.

Proof. Using the previous proposition, there is a constant c satisfying

$$\underbrace{2^{2^{\cdots^2}}}_{n \text{ terms}} \equiv c \pmod{n\phi(n)}. \tag{2.63}$$

By the definition, $2^c \equiv \underbrace{2^{2^{\cdots^2}}}_{n+1 \text{ terms}} \equiv c \pmod{n}$. So c can be a desired m. □

We can replace "2" in this problem into any positive integer. And this proof works on other equations such as $a_n = 3 \cdot 2^{a_{n-1}}$ or $a_n = 2^{a_{n-1}} + 3^{a_{n-1}}$ or $a_n = 2^{2^{a_{n-1}}}$ (replace $\phi(n)$ into $\phi(\phi(n))$). From this, we get a generalized corollary.

Corollary 2.5.2. *For an arbitrary positive integer n, there exists an integer m such that $f(m)$ is integer, where $f(n)$ is*

$$\frac{a \cdot b^m - m}{n} \tag{2.64}$$

or

$$\frac{a_1^m + \cdots + a_k^m - m}{n} \tag{2.65}$$

or

$$\frac{2^{2^m} - m}{n} \tag{2.66}$$

for integers $a, b, a_1, \cdots, a_k$.

Proof is same as the one for the last Proposition. However, this method doesn't work for Original Shortlisted problem.

First 50 constants for $a_n = 2^{a_{n-1}}$ are 0, 0, 1, 0, 1, 4, 2, 0, 7, 6, 9, 4, 3, 2, 1, 0, 1, 16, 5, 16, 16, 20, 6, 16, 11, 16, 7, 16, 25, 16, 2, 0, 31, 18, 16, 16, 9, 24, 16, 16, 18, 16, 4, 20, 16, 6, 17, 16, 23, 36.

Notice that 16 appears very often in first 200 constants and the trend continues.

If we return to the problem D5, following question may be of some interest: what is the smallest integer k for which $a_k \equiv a_{k+1} \equiv \ldots \pmod{100}$? According to D5 problem statement, $k \le n-1$ (and clearly, k is a function of n). As shown in [1], bound can be improved to $k \le \lceil \log_2 n \rceil$. In the same book, reader can find further analysis concerning these lower bounds.

Remark 2.5.1 (Numerical data)**.** *Numerical examples of this congruences convergence are available in [3] sequences A133612-A133619 (submitted by Daniel Geisler).*

Remark 2.5.2 (Ackermann function)**.** *In the theory of hyper-operators, power towers (iterated exponentials like those in problems we observed) are often regarded as the fourth hyperoperator (more precisely, first hyper-operator after exponentiation) and called tetration. Inductively, n^{th} hyper-operator is defined as iterated $(n-1)^{st}$ hyper-operator . The theory of hyper-operators is closely related to so-called Ackermann function, which is defined in the following manner:*

Definition 2.5.2. *For positive integers i, j, Ackermann function $A(i, j)$ is defined as*

$$A(i,j) = \begin{cases} j+1 & \textit{if } i = 0 \\ A(i-1,1) & \textit{if } i > 0, j = 0 \\ A(i-1, A(i, j-1)) & \textit{if } i > 0, j > 0 \end{cases} \tag{2.67}$$

Froemke and Grossman in their paper [2] define (standard) mod-n Ackermann function as:

Definition 2.5.3. *For positive integers i, j, standard mod-n Ackermann function $A_n(i, j)$ is defined as*

$$A_n(i,j) = \begin{cases} j+1 \pmod n & \textit{if } i = 0 \\ A_n(i-1,1) & \textit{if } i > 0, j = 0 \\ A_n(i-1, A(i, j-1)) & \textit{if } i > 0, j > 0 \end{cases} \tag{2.68}$$

where n is a positive integer.

Close relations between Ackermann's function and hyper-operators (Ackermann function can be represented in hyper-operator form as $A(m, n) = hyper(2, m, n + 3) - 3$ - we will not go into details, more information can be found in specialised literature) lead to interesting questions: do the sequences of pentations, hexations, etc. eventually become constant? Does the mod-n Ackermann function eventually become constant? The latter question has been analyzed in [2], with an interesting result: the conjecture that the mod-n Ackermann eventually becomes constant for each n holds for all $n < 4,000,000$ with a surprising unique exception: $n = 1969$. For more information, see [2] and [3] sequence A085119.

References and Further Reading

1 *K. S. Kedlaya, B. Poonen, R. Vakil : "The William Lowell Putnam Mathematical Competition 1985 2000 Problems, Solutions, and Commentary", MAA 2002.*

2 *J. Froemke, J W. Grossman : "A mod-n Ackermann Function, or What's So Special about 1969?", The American Mathematical Monthly 100 (1993).*

3 *N.J.A. Sloane: The Online Encyclopedia of Integer Sequences,* `http://www.research.att.com/~njas/sequences/Seis.html`.

4 *MathLinks Forums,* `http://www.mathlinks.ro/viewtopic.php?t=15089`.

2.6 Using Quadratic Residues

Ho Chung Siu

6 PEN C2 The positive integers a and b are such that the numbers $15a+16b$ and $16a-15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

First Solution. Suppose $15a+16b=x^2$ and $16a-15b=y^2$, where x, y are positive integers. Solving this system of equations, we have

$$a=\frac{15x^2+16y^2}{15^2+16^2}=\frac{15x^2+16y^2}{13\cdot 37},\ b=\frac{16x^2-15y^2}{15^2+16^2}=\frac{16x^2-15y^2}{13\cdot 37}.$$

which implies that

$$15x^2+16y^2\equiv 0\ (mod\ 13\cdot 37)\ \text{ and }\ 16x^2-15y^2\equiv 0\ (mod\ 13\cdot 37)$$

This is equivalent to

$$\begin{cases}15x^2+16y^2\equiv 0\ (mod\ 13)\\ 16x^2-15y^2\equiv 0\ (mod\ 13)\end{cases}\quad\text{and}\quad\begin{cases}15x^2+16y^2\equiv 0\ (mod\ 37)\\ 16x^2-15y^2\equiv 0\ (mod\ 37)\end{cases}$$

Claim 2.6.1. $x,y\equiv 0\ (mod\ 13\cdot 37)$

Once we have this claim, we see that $481\mid x$ and $481\mid y$ (Note that $481=13\cdot 37$). Let us try to see if there is any solution for a,b if $x=y=481$. It suffices to plug in the formula for x,y above. In this case, we are lucky that $(x,y)=(481,481)$ yields a solution $(a,b)=(14911,481)$. Therefore the answer for this question is $\boxed{481^2}$.

It now suffices to show the claim. We will provide several methods:

Method 1. We first use Brahmagupta-Fibonacci Identity:

$$\left(A^2+B^2\right)\left(X^2+Y^2\right)=\left(AX+BY\right)^2+\left(AY-BX\right)^2.$$

From the identity we obtain:

$$\left(15^2+16^2\right)\left(a^2+b^2\right)=\left(15a+16b\right)^2+\left(16a-15b\right)^2=x^4+y^4.$$

Since $15^2+16^2=13\cdot 37$, we have $13\cdot 37\mid x^4+y^4$. It then suffices to apply the following proposition for $p=13$ and $p=37$ to conclude that $x,y\equiv 0\ (mod\ 13)$ and $x,y\equiv 0\ (mod\ 37)$. Since 13 and 37 are relatively prime, we conclude that $x,y\equiv 0\ (mod\ 13\cdot 37)$.

Proposition 2.6.1. *Let p be a prime with $p\equiv 5\ (mod\ 8)$. Suppose that x^4+y^4 is divisible by p for some integers x and y. Then both x, y are divisible by p.*

Proof. Assume for contrary that at least one of them are not divisible by p. Since p divides x^4+y^4, we see that none of them are divisible by p. Fermat's Little Theorem yields that $x^{p-1} \equiv y^{p-1} \equiv 1\ (mod\ p)$. Since $p \equiv 5\ (mod\ 8)$, we have that $\frac{p-1}{4}$ is odd, so $(-1)^{\frac{p-1}{4}} = -1$. Since p divides x^4+y^4, we obtain

$$x^4 \equiv -y^4\ (mod\, p).$$

Raise both sides of the congruence to the power $\frac{p-1}{4}$ to obtain

$$x^{p-1} \equiv (-1)^{\frac{p-1}{4}} y^{p-1} \equiv -y^{p-1}\ (mod\, p).$$

or

$$1 \equiv x^{p-1} \equiv -y^{p-1} \equiv -1\ (mod\, p).$$

which is a contradiction since p is an odd prime. Therefore both x and y are divisible by p. □

Method 2. This method is similar to Method 1, except that we use a different way to conclude

$$13 \cdot 37 \mid x^4 + y^4$$

We first work on the field $\mathbb{Z}/13\mathbb{Z}$ (This is a field since 13 is a prime). Then the system of congruence $15x^2 + 16y^2 \equiv 0\ (mod\ 13)$ and $16x^2 - 15y^2 \equiv 0\ (mod\ 13)$ becomes

$$\begin{bmatrix} x^2 & y^2 \\ -y^2 & x^2 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since the vector $\begin{bmatrix} 15 \\ 16 \end{bmatrix}$ is nonzero in $\mathbb{Z}/13\mathbb{Z}$, this implies that $\begin{bmatrix} x^2 & y^2 \\ -y^2 & x^2 \end{bmatrix}$ has zero determinant so that $x^4 + y^4 = 0$ in $\mathbb{Z}/13\mathbb{Z}$, or equivalently $x^4 + y^4 \equiv 0\ (mod\ 13)$.
Similarly, we can work on the field $\mathbb{Z}/37\mathbb{Z}$, and repeat the argument above. We can then obtain $x^4 + y^4 \equiv 0\ (mod\ 37)$. We can then proceed as in Method 1, using Fermat's Little Theorem.

Method 3. Another method is to use the quadratic reciprocity law. We first recall some of the results that are going to be used here:

Proposition 2.6.2. *Let p, q be odd primes. Then we have the following properties of Legendre symbols:*

1.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for integers a,b.

2.

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

3.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

4.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

We first work with modulo 13. We have the congruence $15x^2 + 16y^2 \equiv 0\ (mod\ 13)$ or equivalently,

$$(4y)^2 \equiv -15x^2\ (mod\ 13)$$

If x is not divisible by 13, there exists an integer x' such that $x'x \equiv 1\ (mod\ 13)$. Multiplying x'^2 to both sides of the congruence above, we get

$$(4yx')^2 \equiv -15 \equiv -2\ (mod\ 13)$$

This means that -2 is a quadratic residue of 13. However if we compute the Legendre symbol,

$$\left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = (-1)^{\frac{13-1}{2}}(-1)^{\frac{13^2-1}{8}} = -1$$

Contradiction. Therefore $x \equiv 0\ (mod\ 13)$. Since $15x^2 + 16y^2 \equiv 0\ (mod\ 13)$, this immediately implies that $y \equiv 0\ (mod\ 13)$ too.
We may apply the same method to the case modulo 37. Then again we proved the claim. □

REFERENCES

1 *PEN Problem C2*, http://www.mathlinks.ro/viewtopic.php?t=150496.

2.7 A Hidden Divisibility

Cosmin Pohoata

7
PEN A13

(AMM, Problem E2510, Saul Singer) Show that for all prime numbers p,

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1}$$

is an integer.

First Solution. It is natural to search for a closed form for $Q(p)$. We see immediately that

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1} = \left(\frac{\prod_{k=1}^{p-1} k^k}{[(p-1)!]^{(p+1)/2}} \right)^2 .$$

Now, the procedure is standard. Using, for example, Legendre's formula (though often atributed to De Polignac; see http://mathworld.wolfram.com/LegendresFormula.html) we can now evaluate the exponent of an arbitrary prime number p in $((p-1)!)^{p+1}$ and prove that it is smaller than the exponent of the same prime p in $\prod_{k=1}^{p-1} k^{2k}$. For a more detailed explanation, we invite the reader to read the second post from [1].

□

Though the problem appeared in the Monthly, as indicated in the cited source, the nice result presented here was given also as a contest problem in the Romanian IMO Team Selection Tests from 1988. It was then suggested by Laurenţiu Panaitopol, who had up is sleeve a magical solution.

Second Solution. We look again (more carefully though) at

$$Q(p) = \prod_{k=1}^{p-1} k^{2k-p-1} = \left(\frac{\prod_{k=1}^{p-1} k^k}{[(p-1)!]^{(p+1)/2}} \right)^2 .$$

We see lots of factorials, but apparently there's nothing we can do with them. So, let's try to avoid them. Here comes the idea. Let's look at

$$Q'(p) = \prod_{k=1}^{p-1} \frac{\binom{p}{k}}{p}.$$

What do we have here? Note that by developing the binomials we get

$$Q'(p) = \prod_{k=1}^{p-1} \frac{\binom{p}{k}}{p} = \frac{[(p-1)!]^{p-1}}{\left(\prod_{k=1}^{p-1} k!\right)\left(\prod_{k=1}^{p-1} (p-k)!\right)} = \frac{[(p-1)!]^{p-1}}{\left(\prod_{k=1}^{p-1} k!\right)^2}.$$

Now we can see the light. Doesn't this last expression look like $Q(p)$? Yes, it does. Just note that the exponents of each $k \in \overline{1, p-1}$ in $[(p-1)!]^{p-1}$, $\left(\prod_{k=1}^{p-1} k!\right)^2$ are $p-1$ and $2(p-k)$, respectively.

This means that

$$\begin{aligned} Q'(p) &= \frac{[(p-1)!]^{p-1}}{\left(\prod_{k=1}^{p-1} k!\right)^2} = \prod_{k=1}^{p-1} k^{2k-p-1} \\ &= Q(p). \end{aligned}$$

Thus, we have settled that

$$Q(p) = \prod_{k=1}^{p-1} \frac{\binom{p}{k}}{p},$$

which is obviously an integer, according to the fact that p divides $\binom{p}{k}$, for all $k \in \overline{1, p-1}$. □

References

1 *PEN Problem A13*, http://www.mathlinks.ro/viewtopic.php?t=150381.

2.8 Fractions Mod p and Wolstenholme's theorem

Daniel Kohen

8
PEN A23
[GhEw pp.104] (Wolstenholme's Theorem)

Prove that if $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}$ is expressed as a fraction, where $p>3$ is a prime, then p^2 divides the numerator.

9
PEN A24
[Putnam 1996] Let $p>3$ be a prime number and $k=\lfloor\frac{2p}{3}\rfloor$ Prove that $\binom{p}{1}+\binom{p}{2}+\cdots+\binom{p}{k}$ is divisible by p^2.

A23. First we will prove some easy elementary facts that will allow us to work with fractions *modp*. This is very useful in some problems but it's not well known. Sometimes, when students are taught congruences they don't think of things such as $k\equiv\frac{1}{2}\pmod{p}$, because it doesn't seem quite natural. But in fact we will see that this makes pefect sense, as long as we are careful that the denominators are relatively prime to the modulus (it's equivalent to the fact that we cannot divide by zero in usual fractions).

Definition 1: Let b and m be integers such that $gcd(b,m)=1$

$$k\equiv\frac{1}{b}\pmod{m}\Longleftrightarrow bk\equiv 1\pmod{m}\tag{2.69}$$

This notation makes perfect sense because k, which is the multplicative inverse of b *modm* exists,since $gcd(b,m)=1$ and it's trivial to see that k is uniquely determined. Moreover the equivalency between both equations is clear when multypling or dividing by b (it can be done since $gcd(b,m)=1$)

When we see something like $\frac{a}{b}$ *modm* with $(b,m)=1$ we can think of the fraction like an integer k which satisfies $bk\equiv a\pmod{m}$

Now we will present the proof of A23

First of all, we can see that that all the denominators are not multiple of p so, as previously showed, we can treat them as integers, so we are left to prove that for $p>3$

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0\pmod{p^2}\tag{2.70}$$

Since $p>3$ is odd, there are an even number of terms in the summation. An useful idea in this kind of problems is to make pairs of numbers in the summation. A natural way of doing this is to sum up the pair of number of the form $\frac{1}{i}$ and $\frac{1}{p-i}$ Then $\frac{1}{i}+\frac{1}{p-i}=\frac{p-i+i}{(p-i)i}=\frac{p}{(p-i)i}$ (I) Since $p>2$

our problem is equivalent to prove that

$$2(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1})\equiv 0\pmod{p^2}\tag{2.71}$$

Using (I) we have to prove that

$$\sum_{i=1}^{p-1} \frac{p}{(p-i)i} \equiv 0 \pmod{p^2} \tag{2.72}$$

Now we get the p factor out;the expression we have to prove is:

$$\sum_{i=1}^{p-1} \frac{1}{(p-i)i} \equiv 0 \pmod{p} \tag{2.73}$$

Now we use that

$$p - i \equiv -i \pmod{p} \Longrightarrow \sum_{i=1}^{p-1} \frac{1}{-i^2} \equiv 0 \pmod{p} \tag{2.74}$$

Since $p > 3$ we can clearly multiply this expression by -1 (We have added a -2 factor to the original equation). Now we have to show that

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \pmod{p} \tag{2.75}$$

Now we are going to replace $\frac{1}{i}$ by its inverse *modp* If a number is the same as its inverse then we have

$$i^2 \equiv 1 \pmod{p} \tag{2.76}$$

So $i \equiv 1 \pmod{p}$ or $i \equiv -1 \pmod{p}$

Now if we consider the numbers $\frac{1}{i}$ with i between 2 and $p-2$ we have an even amount of numbers, each of whom has an inverse in that interval. As a conclusion the equation (6) can be rewritten as:

$$\sum_{i=1}^{p-1} i^2 \equiv 0 \pmod{p} \tag{2.77}$$

Luckily there is a closed form for calculating the sum of the first n squares, which can be easily proved by straightforward induction.

$$\sum_{i=1}^{p-1} i^2 = \frac{p(p+1)(2p+1)}{6} \equiv 0 \pmod{p} \tag{2.78}$$

(Since $p > 3$, 6 is relatively prime to p) That finishes the proof of the problem. □

This theorem, and the technique used to solve them,is very useful in lots of problems,for example, Iberoamerican 2005 problem 3 and APMO 2006 problem 3. The reader might be interested in solving this problems without this ideas and find how difficult they are. However, using fractions *modp* and the ideas used to solve A23, they will find that they are not so difflcult problems. In addition problem 4 of IMO 2005 was a lot easier if the contestant was used to fractions *modp*. This examples shows that this idea, despite the fact that it is very simple, allows to us to tackle some tough problems.

Now we will provide a proof for A24, and in the way we will find an easy generalization for A32 (IMO 1979 problem 1)

A 24. First we state A32 [IMO 1979/1] Let a and b be natural numbers such that

$$\frac{a}{b} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319} \tag{2.79}$$

Prove that a is divisible by 1979

We will rewrite the statement of A24 as

$$\sum_{i=1}^{k} \frac{(p-1)!p}{(p-i)!i!} \equiv 0 \pmod{p^2} \tag{2.80}$$

We get rid of the p in the summation and we have to prove that

$$\sum_{i=1}^{k} \frac{(p-1)!}{(p-i)!i!} \equiv 0 \pmod{p} \tag{2.81}$$

Now we compute

$$\frac{(p-1)!}{(p-i)!} = (p-i+1)(p-i+2)\cdots(p-1) \tag{2.82}$$

And

$$p - i + j \equiv (-1)(i-j) \pmod{p} \tag{2.83}$$

Putting (13) and (14) into (12) $\Longrightarrow$

$$\sum_{i=1}^{k} \frac{((-1)^{i-1})(i-1)!}{i!} \equiv 0 \pmod{p} \Longrightarrow \sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} \equiv 0 \pmod{p} \tag{2.84}$$

Since 1979 is a prime, and in this case $k = 1319$, we find that the statement of A32 is equivalent to showing the generalization provided by (15) Now we will continue our proof. Since $p > 3$, $p = 6l + 1$ or $p = 6l - 1$

Case 1) $p = 6l + 1 \Longrightarrow k = 4l$

$$\sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} = (\sum_{i=1}^{4l} \frac{1}{i}) - 2(\sum_{i=1}^{2l} \frac{1}{2i}) = (\sum_{i=1}^{4l} \frac{1}{i}) - (\sum_{i=1}^{2l} \frac{1}{i}) = (\sum_{i=2l+1}^{4l} \frac{1}{i}) \tag{2.85}$$

Now, as previosuly done in A23, we will make pair of numbers of the form $\frac{1}{2l+t}$ and $\frac{1}{4l+1-t} \Longrightarrow$

$$\frac{1}{2l+t} + \frac{1}{4l+1-t} = \frac{2l+t+4l+1-t}{(4l+1-t)(2l+t)} = \frac{6l+1}{(4l+1-t)(2l+t)} = \frac{p}{(4l+1-t)(2l+t)} \tag{2.86}$$

Since the range of t is the numbers between 1 and l, the denominators are relatively prime to p. Moreover, each term of the form $\frac{1}{2l+t}$ has a pair which forms a multiple of p in equation (16), so 16 can be rewritten as

$$\sum_{i=2l+1}^{4l} \frac{1}{i} = (\frac{1}{2l+1} + \frac{1}{4l}) + (\frac{1}{2l+2} + \frac{1}{4l-1}) + \cdots + (\frac{1}{3l} + \frac{1}{3l+1}) \tag{2.87}$$

Every pair of number in the parenthesis have a sum $\equiv 0 \pmod{p}$ so the whole summation is a multiple of p, finishing the proof.

Case 2) $p = 6l - 1 \Longrightarrow k = 4l - 1$

$$\sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} = (\sum_{i=1}^{4l-1} \frac{1}{i}) - 2(\sum_{i=1}^{2l-1} \frac{1}{2i}) = (\sum_{i=1}^{4l-1} \frac{1}{i}) - (\sum_{i=1}^{2l-1} \frac{1}{i}) = (\sum_{i=2l}^{4l-1} \frac{1}{i}) \tag{2.88}$$

Again we rewrite this as

$$\sum_{i=2l}^{4l-1} \frac{1}{i} = (\frac{1}{2l} + \frac{1}{4l-1}) + (\frac{1}{2l+1} + \frac{1}{4l-2}) + \cdots + (\frac{1}{3l-1} + \frac{1}{3l}) \tag{2.89}$$

Each of the pairs between parenthesis is a multiple of p because

$$\frac{1}{2l-1+t} + \frac{1}{4l-t} = \frac{2l-1+t+4l-t}{(2l-1+t)(4l-t)} = \frac{6l-1}{(2l-1+t)(4l-t)} = \frac{p}{(2l-1+t)(4l-t)} \tag{2.90}$$

This hold for t between 1 and l, and the denominators are clearly relatively prime to p Since all

the terms between parenthesis are a multiple of p the whole summation is a multiple of p and the problem is finished. □

References

1 *PEN Problem A23*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150391.

2 *PEN Problem A24*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150392.

3 *PEN Problem A32*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150400.

4 *Problems suggested* http://www.mathlinks.ro/Forum/resources.php.

2.9 A binomial sum divisible by primes

Darij Grinberg

10
PEN E16

(MM, Problem 1392, George Andrews) Prove that for any prime p in the interval $\left]n, \frac{4n}{3}\right]$, p divides

$$\sum_{j=0}^{n} \binom{n}{j}^4 .$$

The problem can be vastly generalized:

Theorem 1. Let ℓ be a positive integer. If n_1, n_2, ..., n_ℓ are positive integers and p is a prime such that $(\ell - 1)(p-1) < \sum_{i=1}^{\ell} n_i$ and $n_i < p$ for every $i \in \{1, 2, ..., \ell\}$, then $p \mid \sum_{j=0}^{p-1} (-1)^{\ell j} \prod_{i=1}^{\ell} \binom{n_i}{j}$.

Before we prove this, we first show some basic facts about binomial coefficients and remainders modulo primes. We recall how we define binomial coefficients:

Definition. The binomial coefficient $\binom{x}{u}$ is defined for all reals x and for all integers u as follows: $\binom{x}{u} = \frac{x \cdot (x-1) \cdot ... \cdot (x-u+1)}{u!}$ if $u \geq 0$, and $\binom{x}{u} = 0$ if $u < 0$.

Note that the empty product evaluates to 1, and $0! = 1$, so this yields

$$\binom{x}{0} = \frac{x \cdot (x-1) \cdot ... \cdot (x-0+1)}{0!} = \frac{\text{empty product}}{0!} = \frac{1}{1} = 1$$

for every $x \in \mathbb{Z}$.

Theorem 2, the upper negation identity. If n is a real, and r is an integer, then $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$.

Proof of Theorem 2. We distinguish two cases: the case $r < 0$ and the case $r \geq 0$.

If $r < 0$, then $\binom{-n}{r} = 0$ and $\binom{n+r-1}{r} = 0$, so that $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$ ensues.

If $r \geq 0$, then, using the definition of binomial coefficients, we have

$$\begin{aligned}\binom{-n}{r} &= \frac{(-n) \cdot (-n-1) \cdot ... \cdot (-n-r+1)}{r!} = (-1)^r \cdot \frac{n \cdot (n+1) \cdot ... \cdot (n+r-1)}{r!} \\ &= (-1)^r \cdot \frac{(n+r-1) \cdot ... \cdot (n+1) \cdot n}{r!} = (-1)^r \cdot \binom{n+r-1}{r}.\end{aligned}$$

Hence, in both cases $r < 0$ and $r \geq 0$, we have established $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$. Thus, $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$ always holds. This proves Theorem 2. □

Theorem 3. If p is a prime, if u and v are two integers such that $u \equiv v \mod p$, and if k is an integer such that $k < p$, then $\binom{u}{k} \equiv \binom{v}{k} \mod p$.

Proof of Theorem 3. If $k < 0$, then $\binom{u}{k} = \binom{v}{k}$ (because $\binom{u}{k} = 0$ and $\binom{v}{k} = 0$), so that Theorem 3 is trivial. Thus, it remains to consider the case $k \geq 0$ only. In this case, $k!$ is coprime with p (since $k! = 1 \cdot 2 \cdot ... \cdot k$, and all numbers 1, 2, ..., k are coprime with p, since p is a prime and $k < p$).

Now, $u \equiv v \mod p$ yields

$$k! \cdot \binom{u}{k} = k! \cdot \frac{u \cdot (u-1) \cdot ... \cdot (u-k+1)}{k!} = u \cdot (u-1) \cdot ... \cdot (u-k+1)$$
$$\equiv v \cdot (v-1) \cdot ... \cdot (v-k+1) = k! \cdot \frac{v \cdot (v-1) \cdot ... \cdot (v-k+1)}{k!} = k! \cdot \binom{v}{k} \mod p.$$

Since $k!$ is coprime with p, we can divide this congruence by $k!$, and thus we get $\binom{u}{k} \equiv \binom{v}{k}$ mod p. Hence, Theorem 3 is proven. □

Finally, a basic property of binomial coefficients:

Theorem 4. For every nonnegative integer n and any integer k, we have $\binom{n}{k} = \binom{n}{n-k}$.

This is known, but it is important not to forget the condition that n is nonnegative (Theorem 4 would not hold without it!).

Now we will reprove an important fact:

Theorem 5. If p is a prime, and $f \in \mathbb{Q}[X]$ is a polynomial of degree $< p-1$ such that $f(j) \in \mathbb{Z}$ for all $j \in \{0, 1, ..., p-1\}$, then $\sum_{j=0}^{p-1} f(j) \equiv 0 \mod p$.

Before we prove Theorem 5, we recall two lemmata:

Theorem 6. If p is a prime and i is an integer satisfying $0 \leq i \leq p-1$, then $\binom{p-1}{i} \equiv (-1)^i \mod p$.

Theorem 7. If N is a positive integer, and f is a polynomial of degree $< N$, then $\sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = 0$.

Theorem 6 appeared as Lemma 1 in [2], post #2. Theorem 7 is a standard result from finite differences theory.

Proof of Theorem 5. Let $N = p-1$. Then, f is a polynomial of degree $< N$ (since f is a polynomial of degree $< p-1$). Thus, Theorem 7 yields $\sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = 0$. Hence,

$$0 = \sum_{j=0}^{N} (-1)^j \binom{N}{j} f(j) = \sum_{j=0}^{p-1} (-1)^j \underbrace{\binom{p-1}{j}}_{\substack{\equiv (-1)^j \mod p \\ \text{by Theorem 6}}} f(j) \equiv \sum_{j=0}^{p-1} \underbrace{(-1)^j (-1)^j}_{\substack{=\left((-1)^j\right)^2 = \left((-1)^2\right)^j \\ = 1^j = 1}} f(j) = \sum_{j=0}^{p-1} f(j) \mod p.$$

This proves Theorem 5. □

Proof of Theorem 1. The condition $(\ell - 1)(p - 1) < \sum_{i=1}^{\ell} n_i$ rewrites as $\ell(p - 1) - (p - 1) < \sum_{i=1}^{\ell} n_i$. Equivalently, $\ell(p - 1) - \sum_{i=1}^{\ell} n_i < p - 1$.

For every $i \in \{1, 2, ..., \ell\}$, we have $p - n_i - 1 \geq 0$, since $n_i < p$ yields $n_i + 1 \leq p$.

For every $i \in \{1, 2, ..., \ell\}$ and every integer j with $0 \leq j < p$, we have

$$\begin{aligned}\binom{n_i}{j} &= \binom{-(-n_i)}{j} = (-1)^j \binom{(-n_i) + j - 1}{j} \qquad \text{(after Theorem 2)}\\ &\equiv (-1)^j \binom{p - n_i + j - 1}{j} \qquad \text{(by Theorem 3, since } (-n_i) + j - 1 \equiv p - n_i + j - 1 \mod p \text{ and } j < p)\\ &= (-1)^j \binom{p - n_i + j - 1}{(p - n_i + j - 1) - j}\\ &\qquad \text{(by Theorem 4, since } p - n_i + j - 1 \text{ is nonnegative, since } p - n_i - 1 \geq 0 \text{ and } j \geq 0)\\ &= (-1)^j \binom{p - n_i + j - 1}{p - n_i - 1} = (-1)^j \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{(p - n_i - 1)!} \mod p.\end{aligned}$$

Hence, for every integer j with $0 \leq j < p$, we have

$$\begin{aligned}\prod_{i=1}^{\ell} \binom{n_i}{j} &\equiv \prod_{i=1}^{\ell} (-1)^j \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{(p - n_i - 1)!} = \left((-1)^j\right)^{\ell} \prod_{i=1}^{\ell} \frac{\prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{(p - n_i - 1)!}\\ &= \left((-1)^j\right)^{\ell} \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{\prod_{i=1}^{\ell} (p - n_i - 1)!} \mod p,\end{aligned}$$

so that

$$\begin{aligned}&\prod_{i=1}^{\ell} (p - n_i - 1)! \cdot (-1)^{\ell j} \prod_{i=1}^{\ell} \binom{n_i}{j}\\ &\equiv \prod_{i=1}^{\ell} (p - n_i - 1)! \cdot \underbrace{(-1)^{\ell j} \cdot \left((-1)^j\right)^{\ell}}_{\substack{=(-1)^{\ell j} \cdot (-1)^{\ell j}\\ =(-1)^{2\ell j} = 1, \text{ since}\\ 2\ell j \text{ is even}}} \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{\prod_{i=1}^{\ell} (p - n_i - 1)!}\\ &= \prod_{i=1}^{\ell} (p - n_i - 1)! \cdot \frac{\prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u)}{\prod_{i=1}^{\ell} (p - n_i - 1)!}\\ &= \prod_{i=1}^{\ell} \prod_{u=0}^{(p-n_i-1)-1} ((p - n_i + j - 1) - u) \mod p. \qquad (2.91)\end{aligned}$$

Now, define a polynomial f in one variable X by

$$f(X)=\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+X-1)-u). \tag{2.92}$$

Then,

$$\deg f=\deg\left(\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+X-1)-u)\right)=\sum_{i=1}^{\ell}\sum_{u=0}^{(p-n_i-1)-1}\underbrace{\deg((p-n_i+X-1)-u)}_{=1}$$
$$=\sum_{i=1}^{\ell}\underbrace{\sum_{u=0}^{(p-n_i-1)-1}1}_{\substack{=(p-n_i-1)\cdot 1\\ =p-n_i-1\\ =p-1-n_i}}=\sum_{i=1}^{\ell}(p-1-n_i)=\underbrace{\sum_{i=1}^{\ell}(p-1)}_{=\ell(p-1)}-\sum_{i=1}^{\ell}n_i=\ell(p-1)-\sum_{i=1}^{\ell}n_i<p-1.$$

In other words, f is a polynomial of degree $<p-1$. Besides, obviously, $f\in\mathbb{Q}[X]$, and we have $f(j)\in\mathbb{Z}$ for all $j\in\{0,1,...,p-1\}$ (since $f\in\mathbb{Z}[X]$). Thus, Theorem 5 yields $\sum\limits_{j=0}^{p-1}f(j)\equiv 0 \mod p$. Thus,

$$0\equiv\sum_{j=0}^{p-1}f(j)=\sum_{j=0}^{p-1}\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+j-1)-u) \qquad \text{(by (2))}$$
$$=\sum_{j=0}^{p-1}\prod_{i=1}^{\ell}(p-n_i-1)!\cdot(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}$$
$$\left(\text{since }\prod_{i=1}^{\ell}\prod_{u=0}^{(p-n_i-1)-1}((p-n_i+j-1)-u)=\prod_{i=1}^{\ell}(p-n_i-1)!\cdot(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}\text{ by (1)}\right)$$
$$=\prod_{i=1}^{\ell}(p-n_i-1)!\cdot\sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j} \mod p.$$

In other words,

$$p\mid\prod_{i=1}^{\ell}(p-n_i-1)!\cdot\sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}. \tag{2.93}$$

For every $i\in\{1,2,...,\ell\}$, the integer $(p-n_i-1)!$ is coprime with p (since $(p-n_i-1)!=1\cdot 2\cdot...\cdot(p-n_i-1)$, and all numbers 1, 2, ..., $p-n_i-1$ are coprime with p because p is a prime and $p-n_i-1<p$). Hence, the product $\prod\limits_{i=1}^{\ell}(p-n_i-1)!$ is also coprime with p. Thus, (3) yields

$$p\mid\sum_{j=0}^{p-1}(-1)^{\ell j}\prod_{i=1}^{\ell}\binom{n_i}{j}.$$

Thus, Theorem 1 is proven. □

Theorem 1 is a rather general result; we can repeatedly specialize it and still get substantial assertions. Here is a quite strong particular case of Theorem 1:

Theorem 8. Let ℓ be an even positive integer. If n_1, n_2, ..., n_ℓ are positive integers and p is a prime such that $(\ell - 1)(p-1) < \sum\limits_{i=1}^{\ell} n_i$ and $n_i < p$ for every $i \in \{1, 2, ..., \ell\}$, then $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$.

Proof of Theorem 8. Theorem 1 yields $p \mid \sum\limits_{j=0}^{p-1} (-1)^{\ell j} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. But ℓ is even, so that ℓj is even for any $j \in \mathbb{Z}$, and thus

$$\sum_{j=0}^{p-1} \underbrace{(-1)^{\ell j}}_{\substack{=1,\text{ since}\\ \ell j \text{ is even}}} \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} 1 \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} \prod_{i=1}^{\ell} \binom{n_i}{j}.$$

Hence, $p \mid \sum\limits_{j=0}^{p-1} (-1)^{\ell j} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$ becomes $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. Therefore, Theorem 8 is proven. □

Specializing further, we arrive at the following result (which is proved in [1], post #2):

Theorem 9. If n and k are positive integers and p is a prime such that $\frac{2k-1}{2k}(p-1) < n < p$, then $p \mid \sum\limits_{j=0}^{n} \binom{n}{j}^{2k}$.

Proof of Theorem 9. Let $\ell = 2k$. Define positive integers n_1, n_2, ..., n_ℓ by $n_i = n$ for every $i \in \{1, 2, ..., \ell\}$. Then, $n_i < p$ for every $i \in \{1, 2, ..., \ell\}$ (since $n_i = n < p$) and

$$(\ell - 1)(p-1) = (2k-1)(p-1) = 2k \cdot \underbrace{\frac{2k-1}{2k}(p-1)}_{<n} < 2kn = \ell n = \sum_{i=1}^{\ell} n = \sum_{i=1}^{\ell} n_i.$$

Hence, Theorem 8 yields $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$. But $\prod\limits_{i=1}^{\ell} \binom{n_i}{j} = \prod\limits_{i=1}^{\ell} \binom{n}{j} = \binom{n}{j}^{\ell} = \binom{n}{j}^{2k}$, and thus

$$\sum_{j=0}^{p-1} \prod_{i=1}^{\ell} \binom{n_i}{j} = \sum_{j=0}^{p-1} \binom{n}{j}^{2k} = \sum_{j=0}^{n} \binom{n}{j}^{2k} + \sum_{j=n+1}^{p-1} \underbrace{\binom{n}{j}}_{\substack{=0,\text{ since}\\ n \geq 0 \text{ and}\\ j>n}}^{2k} \qquad (\text{since } n < p)$$

$$= \sum_{j=0}^{n} \binom{n}{j}^{2k} + \underbrace{\sum_{j=n+1}^{p-1} 0^{2k}}_{=0} = \sum_{j=0}^{n} \binom{n}{j}^{2k}.$$

Therefore, $p \mid \sum\limits_{j=0}^{p-1} \prod\limits_{i=1}^{\ell} \binom{n_i}{j}$ becomes $p \mid \sum\limits_{j=0}^{n} \binom{n}{j}^{2k}$. Hence, Theorem 9 is proven. □

The problem quickly follows from Theorem 9 in the particular case $k = 2$.

REFERENCES

1 *PEN Problem E16*, http://www.mathlinks.ro/viewtopic.php?t=150539.

2 *PEN Problem A24*, http://www.mathlinks.ro/viewtopic.php?t=150392.

2.10 Sequences of Consecutive Integers

Harun Siljak

11

PEN A37 If n is a natural number, prove that the number $(n+1)(n+2)\cdots(n+10)$ is not a perfect square.

12

PEN A9 Prove that among any ten consecutive positive integers at least one is relatively prime to the product of the others.

13

PEN O51 Prove the among 16 consecutive integers it is always possible to find one which is relatively prime to all the rest.

In the first part of this article, we shall show solutions for the problems. After that, historical background and connection between these problems will be shown. In the end, their generalizations and known results will be given.

Solution-A37. We will assume the contrary, i.e. this product (denote it with A) can be a square. Amongst the numbers $n+1, n+2, \dots, n+10$ at most 4 numbers are divisible by 5 or 7. Among the observed integers there are also at least 6 numbers of the form $2^\alpha 3^\beta c$ where all prime factors of c are greater than 10. It implies that c is a perfect square, so these 6 numbers have the form $2^\alpha 3^\beta k^2$. Now, the possible parity combinations of α, β are
1. α even, β even
2. α even, β odd
3. α odd, β even
4. α odd, β odd
Pigeonhole principle implies that at least two of these numbers have the same parity scheme:
1. In this case two of observed numbers have to be perfect squares, and since $(x+1)^2 - x^2 = 2x+1$ one of these squares has to be $2^2, 3^2$ or 4^2. In each case A is not a perfect square.

2. In this case among the numbers $n+1, n+2, \dots, n+10$ two have the form $3x^2$ and $3y^2$, and since for $x > y$ inequality $|3x^2 - 3y^2| \geq 3(y+1)^2 - 3y^2 = 3(2y+1)$ holds, so $y = 1$ which does not make A a perfect square. □

Solution-A9 Tom Lovering [TL.] Clearly the only common prime factors amongst 10 consecutive positive integers will be $2, 3, 5, 7$.

5 of them will be divisible by 2, at least one of which must also be divisible by 3 and at least one of which must also be divisible by 5, and, if two of the numbers are divisible by 7, one of them will be even.

This leaves two multiples of 3, one multiple of 5, and one multiple of 7 unaccounted for, which makes 4 more of our integers.

But this still leaves one integer not divisible by $2, 3, 5, 7$, and therefore coprime with all other integers of the set, and so coprime with their product. □

Solution-O51 Tomek Kobos [TK.] Let A be the arbitrary set of 16 consecutive integers. It is clear that if p is a common prime factor of two elements of A then $p \in \{2, 3, 5, 7, 11, 13\}$. Thus, it is enough to show that we can find an element of A which is not divisible by any number from this set. Consider the following residues mod 30: $1, 7, 11, 13, 17, 19, 23, 29$. They are coprime with 30 and note that no matter how we choose the 16 consecutive residues there are always 4 of them belonging to this set. The difference between two of this numbers is never divisible by 7 and 13 and the only differences divisible by 11 are $23 - 1 = 22 = 29 - 7$ but this numbers are too far of each other to be in the same set of 16 consecutive integers. Hence among those 4 numbers there is at most one number divisible by 7, at most one number divisible by 11 and at most one number divisible by 13, so we can choose a number which is not divisible by any of them and since this number is also coprime to 30 we are done. □

It is not hard to see the connection between A9 and O51, but how are they related to A37? Well, some of our readers may be tempted to use the result proven in A9 to prove the claim in problem A37. That is one of the methods Indian number theorist Subbayya Sivasankaranarayana Pillai used in his efforts to prove this general result:

Proposition 2.10.1 (Erdos-Selfridge Theorem). *Product of consecutive integers is never a power.*

Pillai made some progress in that field, and the reader can see his conclusions in [P2] (remark: many interesting facts, theorems and their proofs can be found in the papers listed at the end of this article, and the reader is strongly encouraged to study them-it is trully wonderful to find such pearls of number theory available online as public domain- to paraphrase Newton, it really helps us keep our balance on the giants' shoulders).

Still, Pillai's methods shown in the article mentioned above aren't efficient in this case. However, in that time it was already proven that a product of at most 202 consecutive integers is not a square (proof given by Seimatsu Narumi in 1917). In 1939, Erdos proved the general claim that product of an arbitrary number of consecutive integers is not a perfect square. We ommited this proof here, but not due to its complexity, but rather due to its length.

Still, the most general claim wasn't proven. Pillai's work on relative primality of consecutive integers had some interesting results apart from the 'product-power problem'. Pillai has first shown that the least number k for which a sequence of k consecutive integers without a number relatively prime to all others exists is 17.

The least example of such a sequence is $2184, 2185, \dots, 2200$, and an infinite number of those sequences can be obtained by adding all numbers in the sequence a multiple of $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$. Pillai conjectured ([P2]) that the following theorem holds:

Proposition 2.10.2. *For every integer $k > 16$ there exists a sequence of k consecutive integers without a number relatively prime to all others.*

The conjecture was later proven by both Alfred Brauer in [AB] and Pillai in [P3]. Both Pillai's and Brauer's proof are interesting as an introduction for a young number theorist to prime number distributions. For more information about finding such sequences, see [SS].

In 1975, Erdos and Selfridge finally published a proof that product of consecutive integers is never a power in [E3]. Due to its complexity, this proof has been omitted here. The reader may find useful the proofs of certain special cases of this theorem, as they are given in [TT].
It seems like the story about these sequences is over, but that is not true. Propositions 1 and 2 have been generalized in various ways, and the mathematicians still seek for proofs of such generalizations. For instance in the work of Yair Caro, the relative primality in sequence 2 was replaced by a condition $\gcd(a, b) = d$, so the Proposition 2 (and its bound 17) was just made a special case for $d = 1$ (more about it in [S1], [S2], [IG]).
Proposition 2 has been generalized for arbitrary arythmetical progressions $a + nd$, which made the original theorem a special case sof $d = 1$. Another variation was made by replacing 'powers' with the so-called 'almost perfect powers'. More about it can be found in T.N. Shorey's papers, available from [SB].

References

Solutions of the problems

1 [TK], Mathlinks forum: *PEN Problem O51.*

2 [TL], Mathlinks forum: *PEN Problem A9.*

3 [SA], Š. Arslanagić, I. Glogić *Zbirka riješenih zadataka sa takmičenja iz matematike učenika srednjih škola u Federaciji Bosne i Hercegovine (1995-2008).*

Proofs of general theorems cited in the article

4 [P1], S. S. Pillai, *On m consecutive integers-I,* Proceedings of the Indian Academy of Sciences Vol 11, 1940, http://www.ias.ac.in/j_archive/proca/11/1/6-12/viewpage.html.

5 [P2], S. S. Pillai, *On m consecutive integers-II,* Proceedings of the Indian Academy of Sciences Vol 11, 1940, http://www.ias.ac.in/j_archive/proca/11/2/73-80/viewpage.html.

6 [P3], S. S. Pillai, *On m consecutive integers-III,* Proceedings of the Indian Academy of Sciences Vol 13, 1941, http://www.ias.ac.in/j_archive/proca/13/6/530-533/viewpage.html.

7 [AB], A. Brauer, *On a property of k consecutive integers,* Bull. Amer. Math. Soc. 47 (1941), http://www.ams.org/bull/1941-47-04/S0002-9904-1941-07455-0/S0002-9904-1941-07455-0.pdf.

8 [TT], V. Bugaenko, K. Kokhas, Y. Abramov, M. Ilyukhina, *Products of consecutive Integers,* Turnir gorodov 2008, http://olympiads.mccme.ru/lktg/2008/1/1-1en.pdf.

9 [E1], P. Erdos, *Note on products of consecutive integers I,* J. London Math. Soc. 14 (1939), http://www.math-inst.hu/~p_erdos/1939-03.pdf.

10 [E2], P. Erdos, *Note on products of consecutive integers II,* J. London Math. Soc. 14 (1939), http://www.math-inst.hu/~p_erdos/1939-04.pdf.

11 [E3], P. Erdos, *Note on products of consecutive integers III,* Indag. Math. 17 (1955), http://www.math-inst.hu/~p_erdos/1955-08.pdf.

12 [SS], N. J. A. Sloane, *A090318,* Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/A090318.

13 [S1], N. Saradha, L. Hajdu, *On a problem of Pillai and its generalizations,* http://www.math.tifr.res.in/~saradha/pillai-LS18.pdf.

14 [S2], N.Saradha, R. Thangadurai, *Pillai's problem on consecutive integers,* Conference on Number Theory and Cryptography at HRI, Allahabad, 2007, http://www.math.tifr.res.in/~saradha/st-proc-r-f2.pdf.

15 [IG], I. Gassko, *Stapled Sequences and Stapling Coverings of Natural Numbers,* EJoC, Vol 3, 1996, http://www.emis.de/journals/EJC/Volume_3/PDF/v3i1r33.pdf.

16 [SB], T.N. Shorey, *Bibliography*, http://www.math.tifr.res.in/~shorey/.