Olympiad Training for Individual Study

Solution Notes for DNY-NTCONSTRUCT

Evan Chen

March 28, 2020
DNY-SOL-NTCONSTRUCT, OTIS*

Contents

§1 USMCA 2019/1

Kelvin the Frog and Alex the Kat are playing a game on an initially empty blackboard. Kelvin begins by writing a digit. Then, the players alternate inserting a digit anywhere into the number currently on the blackboard, including possibly a leading zero (e.g. 12 can become 123, 142, 512, 012, etc.). Alex wins if the blackboard shows a perfect square at any time, and Kelvin's goal is prevent Alex from winning. Does Alex have a winning strategy?

The answer is no, Kelvin can prevent a perfect square from ever appearing. There are several strategies; here is one.

Claim — Kelvin wins by initially writing the number 7, and then always adding either 7 or 8 to the end.

Proof. Alex clearly can't win on his first turn. Now, suppose that Alex leaves the number $A > 1$ on the board on his nth turn; we contend that Kelvin can prevent Alex from leaving a square on his $(n+1)$st turn as well.

Indeed, if Kelvin writes 7 or 8 as advertised, then he gets either $10A+7$ or $10A+8$. As no square ends in 7 or 8, the only way Alex could win on his $(n+1)$st turn is if $100A+70+d_7$ was a square, or $100A+80+d_8$ was a square. But no two squares exceeding 100 can differ by less than 20, so one of these cases is winning for Kelvin. □

Remark. As $876^2 = 767376$, it is not possible to simply insert 7's in every other digit.

§2 USAMO 2017/1

Prove that there exist infinitely many pairs of relatively prime positive integers $a, b > 1$ for which $a+b$ divides $a^b + b^a$.

One construction: let $d \equiv 1 \pmod 4$, $d > 1$. Let $x = \frac{d^d+2^d}{d+2}$. Then set

$$a = \frac{x+d}{2}, \qquad b = \frac{x-d}{2}.$$

To see this works, first check that b is odd and a is even. Let $d = a-b$ be odd. Then:

$$\begin{aligned} a+b \mid a^b+b^a &\iff (-b)^b + b^a \equiv 0 \pmod{a+b} \\ &\iff b^{a-b} \equiv 1 \pmod{a+b} \\ &\iff b^d \equiv 1 \pmod{d+2b} \\ &\iff (-2)^d \equiv d^d \pmod{d+2b} \\ &\iff d+2b \mid d^d + 2^d. \end{aligned}$$

So it would be enough that

$$d + 2b = \frac{d^d+2^d}{d+2} \implies b = \frac{1}{2}\left(\frac{d^d+2^d}{d+2} - d\right)$$

which is what we constructed. Also, since $\gcd(x, d) = 1$ it follows $\gcd(a, b) = \gcd(d, b) = 1$.

> **Remark.** Ryan Kim points out that in fact, $(a, b) = (2n - 1, 2n + 1)$ is always a solution.

§3 Shortlist 2007 N2

Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

Just let $k = b^2$, so $b \equiv C^n \pmod{b^2}$. Hence $C^n = b(bx + 1)$, but $\gcd(b, bx + 1) = 1$ so $b = A^n$ for some A.

§4 APMO 2009/4

Prove that for any positive integer n, there exists an arithmetic progression

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \dots, \quad \frac{a_n}{b_n}$$

of rational numbers, such that the $2n$ numbers $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are pairwise distinct, and moreover $\gcd(a_i, b_i) = 1$ for every i.

Let $d = p_1 \dots p_n$ be the product of n primes, each prime larger than n. Then select an x with $x \equiv -i \pmod{p_i}$, for $i = 1, \dots, n$, and with x large in terms of d.

Consider the progression

$$\frac{x+1}{d}, \frac{x+2}{d}, \dots, \frac{x+n}{d}.$$

We claim it works.

Then, in the first fraction p_1 cancels from both the numerator and denominator, and that is the only cancellation (since $p_1 > n$). In general, the reduced ith fraction has

$$\begin{aligned} a_i &= \frac{x+i}{p_i} \\ b_i &= \frac{d}{p_i} = p_1 \dots p_{i-1} p_{i+1} \dots p_n. \end{aligned}$$

Obviously b_i and a_i are pairwise distinct. Moreover if x is large enough, then $a_i > d$ for all i while $b_i < d$ for all i. This completes the proof.

§5 Shortlist 2017 N2

Let p be a fixed prime number. Ankan and Ryan play the following turn-based game, with Ankan moving first. On their turn, each player selects an index $i \in \{0, \dots, p-1\}$ not chosen on a previous turn, and a digit $a_i \in \{0, \dots, 9\}$. This continues until all indices have been chosen (hence for p turns). Then, Ankan wins if the number

$$N = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_{p-1} 10^{p-1}$$

is divisible by p; otherwise Ryan wins. For each prime p, determine which player has the winning strategy.

The first player Ankan can always win.

Assume first $\gcd(p, 10) = 1$, and let e be the order of $10 \pmod p$. Ankan begins by choosing $a_{p-1} = 0$.

Now let $p - 1 = de$. We consider two cases:

- If e is even, then $10^{e/2} \equiv -1 \pmod p$. Ankan imagines pairing the indices $\{0, 1, \dots, p-2\}$ into pairs which differ by $e/2$ in the obvious way (there are d pairs of 2 each). Now whenever Ryan picks a number a_i, Ankan selects the corresponding index j and sets $a_j = a_i$. As $10^j a_j + 10^i a_i \equiv 0 \pmod p$ this strategy wins.

- If e is odd, then d must be even. Ankan imagines pairing the indices $\{0, 1, \dots, p-2\}$ into pairs which differ by e in the obvious way (there are $d/2$ pairs of 2 each). Now whenever Ryan picks a number a_i Ankan selects the corresponding index j and sets $a_j = 9 - a_i$. Thus $10^j a_j + 10^i a_i \equiv 9 \cdot 10^i \pmod p$. So the final number is a multiple of $9 \dots 9 = 10^e - 1$ which is divisible by p.

If $p = 2$ or $p = 5$, Ankan just picks $a_0 = 0$ and wins. Thus Ankan has the winning strategy.

> **Remark.** One can phrase this solution without the use of orders d and e; it's merely casework on the value of $10^{\frac{1}{2}(p-1)}$.

§6 China 2019/2

A *Pythagorean triple* is a set of three distinct positive integers $\{a, b, c\}$ which satisfies $a^2 + b^2 = c^2$. Prove that if P and Q are Pythagorean triples then there exists a finite sequence $P_0, \dots, P_n$ of Pythagorean triples satisfying $P = P_0$, $Q = P_n$, and $P_i \cap P_{i+1} \neq \varnothing$ for each $i = 0, \dots, n-1$.

Write $P \sim Q$ if $P \cap Q \neq \varnothing$. We say P and Q are *connected* if there exists a path as in the problem statement. Both these relations are obviously mutual.

We denote the triple $\{3n, 4n, 5n\}$ by $B(n)$. Note every Pythagorean triple has an element divisible by 4 (by looking modulo 8), hence intersects some $B(n)$. Thus it suffices to show that $B(n)$ is connected to $B(1)$ for every n.

> **Claim** — The triples $B(n)$ and $B(2n)$ are connected for any integer $n > 0$.

Proof. We have

$$\begin{aligned} B(2n) = \{6n, 8n, 10n\} &\sim \{8n, 15n, 17n\} \sim \{9n, 12n, 15n\} \\ &\sim \{5n, 12n, 13n\} \sim \{3n, 4n, 5n\} = B(n). \square \end{aligned}$$

> **Claim** — Let $p > 0$ be an odd integer, and $d > 0$ any integer. Then $B(dp)$ and $B\left(d \cdot \frac{p^2-1}{2}\right)$ are connected.

Proof. We have

$$\begin{aligned} B(p) = \{d \cdot 3p, d \cdot 4p, d \cdot 5p\} &\sim \{d \cdot 4p, d \cdot 2(p^2-1), d \cdot 2(p^2+1)\} \\ &\sim \left\{d \cdot 3 \cdot \frac{p^2-1}{2}, d \cdot 4 \cdot \frac{p^2-1}{2}, d \cdot 5 \cdot \frac{p^2-1}{2}\right\} \\ &= B\left(d \cdot \frac{p^2-1}{2}\right). \square \end{aligned}$$

Indeed, let n be any integer. IF n is even then $B(n)$ is connected to $B(n/2)$. Else if $p > 2$ is the *largest* prime factor of n, then $B(n)$ is connected to $B(n/p \cdot \frac{p^2-1}{2})$.

We claim that if we repeat this procedure, then eventually each $B(n)$ arrives at $B(1)$. Indeed, define the *complexity* of n to be the ordered pair $(p, \nu_p(n))$; then the complexity of n decreases lexicographically as we iterate the above procedure.

§7 (No source)

Let $a_1, \dots, a_{100}$ be positive integers. Let P be a polynomial with integer coefficients such that $P(n)$ divides $a_1^n + a_2^n + \dots + a_{100}^n$ for $n = 1, 2, \dots$. Must P be constant?

The answer is yes, P must be constant.

By Schur's theorem, we can find some integer b and some prime $p > 100 + \max_i a_i$ such that $P(b) \equiv 0 \pmod p$.

Now pick n with

$$\begin{aligned} n &\equiv 0 \pmod{p-1} \\ n &\equiv b \pmod{p}. \end{aligned}$$

For this n, we have $P(b) \equiv P(n) \equiv 0 \pmod p$, and $\sum_i a_i^n \equiv \sum_i 1 \equiv 100 \pmod p$. This is a contradiction.

§8 BAMO 2011/5

Decide whether there exists a row of Pascal's triangle containing four pairwise distinct numbers a, b, c, d such that $a = 2b$ and $c = 2d$.

An example is $\binom{203}{68} = 2\binom{203}{67}$ and $\binom{203}{85} = 2\binom{203}{83}$.

To get this, the idea is to look for two adjacent entries and two entries off by one, and solving the corresponding equations. The first one is simple:

$$\binom{n}{j} = 2\binom{n}{j-1} \implies n = 3j - 1.$$

The second one is more involved:

$$\begin{aligned} \binom{n}{k} &= 2\binom{n}{k-2} \\ \implies (n-k+1)(n-k+2) &= 2k(k-1) \\ \implies 4(n-k+1)(n-k+2) &= 8k(k-1) \\ \implies (2n-2k+3)^2 - 1 &= 2\left((2k-1)^2 - 1\right) \\ \implies (2n-2k+3)^2 - 2(2k-1)^2 &= -1 \end{aligned}$$

Using standard methods for the Pell equation:

- $(7+5\sqrt{2})(3+2\sqrt{2}) = 41+29\sqrt{2}$. So $k=15$, $n=34$, doesn't work.
- $(41+29\sqrt{2})(3+2\sqrt{2}) = 239+169\sqrt{2}$. Then $k=85$, $n=203$.

§9 TSTST 2012/5

A rational number x is given. Prove that there exists a sequence $x_0, x_1, x_2, \dots$ of rational numbers with the following properties:

(a) $x_0 = x$;

(b) for every $n \ge 1$, either $x_n = 2x_{n-1}$ or $x_n = 2x_{n-1} + \frac{1}{n}$;

(c) x_n is an integer for some n.

Think of the sequence as a process over time. We'll show that:

> **Claim** — At any given time t, if the denominator of x_t is some odd prime power $q = p^e$, then we can delete a factor of p from the denominator, while only adding powers of two to the denominator.

(Thus we can just delete off all the odd primes one by one and then double appropriately many times.)

Proof. The idea is to add only fractions of the form $(2^k q)^{-1}$.

Indeed, let n be large, and suppose $t < 2^{r+1}q < 2^{r+2}q < \dots < 2^{r+m}q < n$. For some binary variables $\varepsilon_i \in \{0,1\}$ we can have

$$x_n = 2^{n-t}x_t + c_1 \cdot \frac{\varepsilon_1}{q} + c_2 \cdot \frac{\varepsilon_2}{q} \cdots + c_s \cdot \frac{\varepsilon_m}{q}$$

where c_i is some power of 2 (to be exact, $c_i = \frac{2^{n-2^{r+i}q}}{2^{r+1}}$, but the exact value doesn't matter).

If m is large enough the set $\{0, c_1\} + \{0, c_2\} + \dots + \{0, c_m\}$ spans everything modulo p. (Actually, Cauchy-Davenport implies $m = p$ is enough, but one can also just use Pigeonhole to notice some residue appears more than p times, for $m = O(p^2)$.) Thus we can eliminate one factor of p from the denominator, as desired. □

§10 Shortlist 2014 N4

Let $n > 1$ be an integer. Prove that there are infinitely many integers $k \ge 1$ such that

$$\left\lfloor \frac{n^k}{k} \right\rfloor$$

is odd.

If n is odd, then we can pick any prime p dividing n, and select $k = p^m$ for sufficiently large integers m.

Now suppose n is even. Choose any integer $e \ge 1$ and let p be an odd prime dividing $n^{2^e} - 2^e$ (since $n^{2^e} \neq 2^{e+1}$). Then

$$n^{2^e p} \equiv 2^e \pmod{2^e p}$$

since $2^e \mid n^{2^e p}$ holds, and also $(n^{2^e})^p \equiv n^{2^e} \equiv 2^e \pmod p$. So that is the remainder.

Then we can take $k = 2^e p$ and then

$$\left\lfloor \frac{n^k}{k} \right\rfloor = \frac{n^k - 2^e}{k}$$

is odd.

§11 USA TST 2007/4

Determine whether or not there exist positive integers a and b such that a does not divide $b^n - n$ for all positive integers n.

The answer is no.

In fact, for any fixed integer b, the sequence

$$b,\ b^b,\ b^{b^b},\ \dots$$

is eventually constant modulo any integer. (This follows by induction on the exponent: for it to be eventually constant modulo a, it is enough to be eventually constant modulo $\varphi(a)$, hence modulo $\varphi(\varphi(a))$, etc.)

Therefore if n is a suitably tall power-tower of b's, then we will have $b^n \equiv n \pmod a$.

§12 China TST 2018/2/4

Let k, M be positive integers such that $k-1$ is not squarefree. Prove that there exists a positive real number α such that $\lfloor \alpha \cdot k^n \rfloor$ and M are relatively prime for any positive integer n.

Let $p^2 \mid k-1$ be prime and let $d = \frac{k-1}{p}$. Consider the number

$$\alpha = N + \frac{1}{p} = N + 0.\overline{ddd\dots}_k$$

in base k. We claim it works for a suitable integer N.

Indeed, we have

$$\lfloor \alpha k^n \rfloor = k^n N + d \cdot \frac{k^n - 1}{k-1} = \left(N + \frac{1}{p}\right) k^n - \frac{1}{p}.$$

If we pick N such that $p \nmid N$, then the middle expression is not divisible by p (since d is divisible by p). Moreover, we can select N such that $q \mid N + p^{-1}$ for every prime $q \mid M$ other than p. Thus the Chinese remainder theorem completes the problem.

> **Remark** (Example)**.** If $k = 10$, and $M = 2 \cdot 3 \cdot 5 \cdot 7$, then one could take $\alpha = 23.33333\dots$.

> **Remark** (Repeating base k mistake)**.** It is tempting to choose $\alpha = N + 0.\overline{ddd\dots}_k$ in general, but one has to be careful in this case that $d \neq k-1$ because this would actually cause $\alpha = N+1$.

§13 EGMO 2018/2

Consider the set

$$A = \left\{ 1 + \frac{1}{k} : k = 1, 2, 3, \dots \right\}.$$

For every integer $x \geq 2$, let $f(x)$ denote the minimum integer such that x can be written as the product of $f(x)$ elements of A (not necessarily distinct). Prove that there are infinitely many pairs of integers $x \geq 2$ and $y \geq 2$ for which

$$f(xy) < f(x) + f(y).$$

One of many constructions: let $n = 2^e + 1$ for $e \equiv 5 \pmod{10}$ and let $x = 11$, $y = n/11$ be our two integers.

We prove two lemmas:

> **Claim** — For any $m \geq 2$ we have $f(m) \geq \lceil \log_2 m \rceil$.

Proof. This is obvious. □

It follows that $f(n) = e + 1$, since $n = \frac{n}{n-1} \cdot 2^e$.

> **Claim** — $f(11) = 5$.

Proof. We have $11 = \frac{33}{32} \cdot \frac{4}{3} \cdot 2^3$. So it suffices to prove $f(11) > 4$.

Note that a decomposition of 11 must contain a fraction at most $\frac{11}{10} = 1.1$. But $2^3 \cdot 1.1 = 8.8 < 11$, contradiction. □

To finish, note that

$$f(11) + f(n/11) \geq 5 + \log_2(n/11) = 1 + \log_2(16n/11) > 1 + e = 1 + f(n).$$

> **Remark.** Most solutions seem to involve picking n such that $f(n)$ is easy to compute. Indeed, it's hard to get nontrivial lower bounds other than the log, and even harder to actually come up with complicated constructions. It might be said the key to this problem is doing as little number theory as possible.

§14 USAMTS 4/3/29

A positive integer is called *uphill* (resp. *downhill*) if the nonzero digits in the decimal representation form a non-decreasing (resp. non-increasing) sequence. (For example, 1148 is uphill, 763 is downhill, 555 is both.) Decide whether each of the following statements is true or false:

(a) If $P(x) \in \mathbb{Q}[x]$ takes integer values for all uphill integers, then it takes integer values for all integers.

(b) If $P(x) \in \mathbb{Q}[x]$ takes integer values for all downhill integers, then it takes integer values for all integers.

The answer to both parts is no.

For the first part, note that uphill integers are the sum of at most nine elements in the set $\{1, 11, 111, 1111, \dots\}$, with repetition. In particular, no uphill integer is $10 \pmod{11}$ and thus

$$P(x) = \frac{(x-10)^{11} - 1}{11}$$

is a counterexample.

The second part is trickier. Here is an outline: show there exists a large integer n and a residue $r \pmod{2^n}$ not achieved by any downhill integer. Then choose

$$P(x) = \frac{(x-r+1)(x-r+2)\dots(x-r+2^n-1)}{2(2^n-1)!}$$

which has $P(r) = \frac{1}{2}$.

§15 USAMO 2006/3

For integral m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence

$$\{p(f(n^2)) - 2n\}_{n \ge 0}$$

is bounded above. (In particular, this requires $f(n^2) \neq 0$ for $n \ge 0$.)

If f is the (possibly empty) product of linear factors of the form $4n - a^2$, then it satisfies the condition. We will prove no other polynomials work. In what follows, assume f is irreducible and nonconstant.

It suffices to show for every positive integer c, there exists a prime p and a nonnegative integer n such that $n \le \frac{p-1}{2} - c$ and p divides $f(n^2)$.

Firstly, recall there are infinitely many odd primes p, with $p > c$, such that p divides some $f(n^2)$, by Schur's Theorem. Looking mod such a p we can find n between 0 and $\frac{p-1}{2}$ (since $n^2 \equiv (-n)^2 \pmod p$). We claim that only finitely many p from this set can fail now. For if a p fails, then its n must be between $\frac{p-1}{2} - c$ and $\frac{p-1}{2}$. That means for some $0 \le k \le c$ we have

$$0 \equiv f\left(\left(\frac{p-1}{2} - k\right)^2\right) \equiv f\left(\left(k + \frac{1}{2}\right)^2\right) \pmod p.$$

There are only finitely many p dividing

$$\prod_{k=1}^{c} f\left(\left(k + \frac{1}{2}\right)^2\right)$$

unless one of the terms in the product is zero; this means that $4n - (2k+1)^2$ divides $f(n)$. This establishes the claim and finishes the problem.

§16 USAMO 2013/5

Let m and n be positive integers. Prove that there exists a positive integer c such that cm and cn have the same nonzero decimal digits.

One-line spoiler: 142857. More verbosely, the idea is to look at the decimal representation of $1/D$, m/D, n/D for a suitable denominator D, which have a "cyclic shift" property in which the digits of n/D are the digits of m/D shifted by 3.

> **Remark** (An example to follow along)**.** Here is an example to follow along in the subsequent proof If $m = 4$ and $n = 23$ then the magic numbers $e = 3$ and $D = 41$ obey
>
> $$10^3 \cdot \frac{4}{41} = 97 + \frac{23}{41}.$$
>
> The idea is that
>
> $$\begin{aligned} \frac{1}{41} &= 0.\overline{02439} \\ \frac{4}{41} &= 0.\overline{09756} \\ \frac{23}{41} &= 0.\overline{56097} \end{aligned}$$
>
> and so $c = 2349$ works; we get $4c = 9756$ and $23c = 56097$ which are cyclic shifts of each other by 3 places (with some leading zeros appended).

Here is the one to use:

> **Claim** — There exists positive integers D and e such that $\gcd(D, 10) = 1$, $D > \max(m, n)$, and moreover
>
> $$\frac{10^e m - n}{D} \in \mathbb{Z}.$$

Proof. Suppose we pick some exponent e and define the number

$$A = 10^e n - m.$$

Let $r = \nu_2(m)$ and $s = \nu_5(m)$. As long as $e > \max(r, s)$ we have $\nu_2(A) = r$ and $\nu_5(A) = s$, too. Now choose any $e > \max(r, s)$ big enough that $A > 2^r 5^s \max(m, n)$ also holds. Then the number $D = \frac{A}{2^r 5^s}$ works; the first two properties hold by construction and

$$10^e \cdot \frac{n}{D} - \frac{m}{D} = \frac{A}{D} = 2^r 5^s$$

is an integer. ☐

> **Remark** (For people who like obscure theorems)**.** Kobayashi's theorem implies we can actually pick D to be prime.

Now we take c to be the number under the bar of $1/D$ (leading zeros removed). Then the decimal representation of $\frac{m}{D}$ is the decimal representation of cm repeated (possibly including leading zeros). Similarly, $\frac{n}{D}$ has the decimal representation of cm repeated (possibly including leading zeros). Finally, since

$$10^e \cdot \frac{m}{D} - \frac{n}{D} \text{ is an integer}$$

it follows that these repeating decimal representations are rotations of each other by e places, so in particular they have the same number of nonzero digits.

> **Remark.** Many students tried to find a D satisfying the stronger hypothesis that $1/D$, $2/D$, ..., $(D-1)/D$ are cyclic shifts of each other. For example, this holds in the famous $D = 7$ case.
>
> The official USAMO 2013 solutions try to do this by proving that 10 is a primitive root modulo 7^e for each $e \ge 1$, by Hensel lifting lemma. I think this argument is actually *incorrect*, because it breaks if either m or n are divisible by 7. Put bluntly, $\frac{7}{49}$ and $\frac{8}{49}$ are not shifts of each other.
>
> One may be tempted to resort to using large primes D rather than powers of 7 to deal with this issue. However it is an open conjecture (a special case of Artin's primitive root conjecture) whether or not $10 \pmod p$ is primitive infinitely often, which is the necessary conjecture so this is harder than it seems.

§17 RMM 2012/4

Prove there are infinitely many integers n such that n does not divide $2^n + 1$, but divides $2^{2^n+1} + 1$.

Zsig hammer! Define the sequence $n_0, n_1, \dots$ as follows. Set $n_0 = 3$, and then for $k \ge 1$ we let $n_k = pn_{k-1}$ where p is a primitive prime divisor of $2^{2^{n_{k-1}}+1} + 1$ (by Zsigmondy). For example, $n_1 = 57$.

This sequence of n_k's works for $k \ge 1$, by construction.

It's very similar to IMO 2000 Problem 5.

§18 IMO 2004/6

We call a positive integer *alternating* if every two consecutive digits in its decimal representation are of different parity. Find all positive integers n which have an alternating multiple.

If $20 \mid n$, then clearly n has no alternating multiple since the last two digits are both even. We will show the other values of n all work.

The construction is just rush-down do-it. The meat of the solution is the two following steps.

> **Claim** (Tail construction) — For every even integer $w \ge 2$,
>
> - there exists an even alternating multiple $g(w)$ of 2^{w+1} with exactly w digits, and
> - there exists an even alternating multiple $h(w)$ of 5^w with exactly w digits.

(One might note this claim is implied by the problem, too.)

Proof. We prove the first point by induction on w. If $w = 2$, take $g(2) = 32$. In general, we can construct $g(w+2)$ from $g(w)$ by adding some element in

$$10^w \cdot \{10, 12, 14, 16, 18, 30, \dots, 98\}$$

to $g(w)$, corresponding to the digits we want to append to the start. This multiple is automatically divisible by 2^{w+1}, and also can take any of the four possible values modulo 2^{w+3}.

The second point is a similar induction, with base case $h(2) = 50$. The same set above consists of numbers divisible by 5^w, and covers all residues modulo 5^{w+2}. Careful readers might recognize the second part as essentially USAMO 2003/1. □

Claim (Head construction) — If $\gcd(n, 10) = 1$, then for any b, there exists an even alternating number $f(b \bmod n)$ which is $b \pmod n$.

Proof. A standard argument shows that

$$10 \cdot \frac{100^m - 1}{99} = \underbrace{1010\dots10}_{m\ 10\text{'s}} \equiv 0 \pmod n$$

for any m divisible by $\varphi(99n)$. Take a very large such m, and then add on b distinct numbers of the form $10^{\varphi(n)r}$ for various even values of r; these all are $1 \pmod n$ and change some of the 1's to 3's. □

Now, we can solve the problem. Consider three cases:

- If $n = 2^k m$ where $\gcd(m, 10) = 1$ and $k \ge 2$ is even, then the concatenated number
$$10^k f\left(-\frac{g(k)}{10^k} \bmod m\right) + g(k)$$
works fine.
- If $n = 5^k m$ where $\gcd(m, 10) = 1$ and $k \ge 2$ is even, then the concatenated number
$$10^k f\left(-\frac{h(k)}{10^k} \bmod m\right) + h(k)$$
works fine.
- If $n = 50m$ where $\gcd(m, 10) = 1$, then the concatenated number
$$100f\left(-\frac{1}{2} \bmod m\right) + 50$$
works fine.

Since every non-multiple of 20 divides such a number, we are done.

§19 USAMO 2012/3

Determine which integers $n > 1$ have the property that there exists an infinite sequence $a_1, a_2, a_3, \dots$ of nonzero integers such that the equality

$$a_k + 2a_{2k} + \cdots + na_{nk} = 0$$

holds for every positive integer k.

Answer: all $n > 2$.

For $n = 2$, we have $a_k + 2a_{2k} = 0$, which is clearly not possible, since it implies $a_{2^k} = \frac{a_1}{2^{k-1}}$ for all $k \geq 1$.

For $n \geq 3$ we will construct a *completely multiplicative* sequence (meaning $a_{ij} = a_i a_j$ for all i and j). Thus (a_i) is determined by its value on primes, and satisfies the condition as long as $a_1 + 2a_2 + \cdots + na_n = 0$. The idea is to take two large primes and use Bezout's theorem, but the details require significant care.

We start by solving the case where $n \geq 9$. In that case, by Bertrand postulate there exists primes p and q such that

$$\lceil n/2 \rceil < q < 2 \lceil n/2 \rceil \quad \text{and} \quad \frac{1}{2}(q-1) < p < q-1.$$

Clearly $p \neq q$, and $q \geq 7$, so $p > 3$. Also, $p < q < n$ but $2q > n$, and $4p \geq 4\left(\frac{1}{2}(q+1)\right) > n$. We now stipulate that $a_r = 1$ for any prime $r \neq p, q$ (in particular including $r = 2$ and $r = 3$). There are now three cases, identical in substance.

- If $p, 2p, 3p \in [1, n]$ then we would like to choose nonzero a_p and a_q such that

$$6p \cdot a_p + q \cdot a_q = 6p + q - \frac{1}{2}n(n+1)$$

  which is possible by Bézout lemma, since $\gcd(6p, q) = 1$.

- Else if $p, 2p \in [1, n]$ then we would like to choose nonzero a_p and a_q such that

$$3p \cdot a_p + q \cdot a_q = 3p + q - \frac{1}{2}n(n+1)$$

  which is possible by Bézout lemma, since $\gcd(3p, q) = 1$.

- Else if $p \in [1, n]$ then we would like to choose nonzero a_p and a_q such that

$$p \cdot a_p + q \cdot a_q = p + q - \frac{1}{2}n(n+1)$$

  which is possible by Bézout lemma, since $\gcd(p, q) = 1$. (This case is actually possible in a few edge cases, for example when $n = 9$, $q = 7$, $p = 5$.)

It remains to resolve the cases where $3 \leq n \leq 8$. We enumerate these cases manually:

- For $n = 3$, let $a_n = (-1)^{\nu_3(n)}$.
- For $n = 4$, let $a_n = (-1)^{\nu_2(n)+\nu_3(n)}$.
- For $n = 5$, let $a_n = (-2)^{\nu_5(n)}$.
- For $n = 6$, let $a_n = 5^{\nu_2(n)} \cdot 3^{\nu_3(n)} \cdot (-42)^{\nu_5(n)}$.
- For $n = 7$, let $a_n = (-3)^{\nu_7(n)}$.
- For $n = 8$, we can choose $(p, q) = (5, 7)$ in the prior construction.

This completes the constructions for all $n > 2$.

§20 TSTST 2016/3

Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \dots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n.

We claim that

$$Q(x) = 420(x^2-1)^2$$

works. Clearly, it suffices to prove the result when $n = 4$ and when n is an odd prime p. The case $n = 4$ is trivial, so assume now $n = p$ is an odd prime.

First, we prove the following easy claim.

Claim — For any odd prime p, there are at least $\frac{1}{2}(p-3)$ values of a for which $\left(\frac{1-a^2}{p}\right) = +1$.

Proof. Note that if $k \neq 0$, $k \neq \pm 1$, $k^2 \neq -1$, then $a = 2(k+k^{-1})^{-1}$ works. Also $a = 0$ works. □

Let $F(x) = (x^2-1)^2$. The range of F modulo p is contained within the $\frac{1}{2}(p+1)$ quadratic residues modulo p. On the other hand, if for some t neither of $1 \pm t$ is a quadratic residue, then t^2 is omitted from the range of F as well. Call such a value of t *useful*, and let N be the number of useful residues. We aim to show $N \geq \frac{1}{4}p - 2$.

We compute a lower bound on the number N of useful t by writing

$$\begin{aligned}
N &= \frac{1}{4}\left(\sum_t \left[\left(1-\left(\frac{1-t}{p}\right)\right)\left(1-\left(\frac{1+t}{p}\right)\right)\right] - \left(1-\left(\frac{2}{p}\right)\right) - \left(1-\left(\frac{-2}{p}\right)\right)\right) \\
&\geq \frac{1}{4}\sum_t \left[\left(1-\left(\frac{1-t}{p}\right)\right)\left(1-\left(\frac{1+t}{p}\right)\right)\right] - 1 \\
&= \frac{1}{4}\left(p + \sum_t \left(\frac{1-t^2}{p}\right)\right) - 1 \\
&\geq \frac{1}{4}\left(p + (+1)\cdot\tfrac{1}{2}(p-3) + 0\cdot 2 + (-1)\cdot\left((p-2)-\tfrac{1}{2}(p-3)\right)\right) - 1 \\
&\geq \frac{1}{4}(p-5).
\end{aligned}$$

Thus, the range of F has size at most

$$\frac{1}{2}(p+1) - \frac{1}{2}N \leq \frac{3}{8}(p+3).$$

This is less than $0.499p$ for any $p \geq 11$.

Remark. In fact, the computation above is essentially an equality. There are only two points where terms are dropped: one, when $p \equiv 3 \pmod 4$ there are no $k^2 = -1$ in the lemma, and secondly, the terms $1-(2/p)$ and $1-(-2/p)$ are dropped in the initial estimate for N. With suitable modifications, one can show that in fact, the range of F is exactly equal to

$$\frac{1}{2}(p+1) - \frac{1}{2}N = \begin{cases} \frac{1}{8}(3p+5) & p \equiv 1 \pmod 8 \\ \frac{1}{8}(3p+7) & p \equiv 3 \pmod 8 \\ \frac{1}{8}(3p+9) & p \equiv 5 \pmod 8 \\ \frac{1}{8}(3p+3) & p \equiv 7 \pmod 8. \end{cases}$$

§21 Shortlist 2013 N4

Determine whether there exists an infinite sequence of nonzero digits a_0, a_1, a_2, a_3, ... such that the number $\overline{a_k a_{k-1} \dots a_1 a_0}$ is a perfect square for all sufficiently large k.

The answer is no.

Assume for contradiction such a sequence exists, and let $x_k = \sqrt{\overline{a_k a_{k-1} \dots a_1 a_0}}$ for k large enough. Difference of squares gives

$$A_k \cdot B_k \overset{\text{def}}{=} (x_{k+1} - x_k)(x_{k+1} + x_k) = a_{k+1} \cdot 10^k$$

with $\gcd(A_k, B_k) = 2\gcd(x_k, x_{k-1})$ since x_k and x_{k-1} have the same parity.

We now split the proof in two cases:

- First assume $\nu_5(x_k^2) = 2e < k$ for some index k. Then we actually need to have

  $$2e = \nu_5(x_k^2) = \nu_5(x_{k+1}^2) = \cdots.$$

  Thus in this situation, we need to have $\min(\nu_5(A_k), \nu_5(B_k)) = e$, and thus $\max(\nu_5(A_k), \nu_5(B_k)) = k - e$. So

  $$\min(A_k, B_k) \ge 5^{k-e}.$$

- Otherwise, assume $\nu_5(x_k^2) \ge k$ for all k. Note in particular that $a_0 = 5$, thus all x_k are always odd. So one of A_k and B_k is divisible by 2^{k-1}. Hence for each k,

  $$\min(A_k, B_k) \ge 2^{k-1} \cdot 5^{k/2}$$

  which is impossible for large enough k.

However, since $A_k B_k = a_{k+1} \cdot 10^k$ we also obviously have $\min(A_k, B_k) < \sqrt{9 \cdot 10^k}$ which is incompatible with both cases above.

§22 EGMO 2014/3

We denote the number of positive divisors of a positive integer m by $d(m)$ and the number of distinct prime divisors of m by $\omega(m)$. Let k be a positive integer. Prove that there exist infinitely many positive integers n such that $\omega(n) = k$ and $d(n)$ does not divide $d(a^2 + b^2)$ for any positive integers a, b satisfying $a + b = n$.

Weird problem. The condition is very artificial, although the construction is kind of fun. I'm guessing the low scores during the actual contest were actually due to an unusually tricky P2.

Let $n = 2^{p-1}t$, where $t \equiv 5 \pmod 6$, $\omega(t) = k-1$, and $p \gg t$ is a sufficiently large prime. Let $a+b=n$ and $a^2+b^2=c$. We claim that $p \nmid d(c)$, which solves the problem since $p \mid d(n)$.

First, note that $3 \nmid a^2+b^2$, since $3 \nmid n$. Next, note that $c < 2n^2 < 5^{p-1}$ (since $p \gg t$) so no exponent of an odd prime in c exceeds $p-2$. Moreover, $c < 2^{3p-1}$.

So, it remains to check that $\nu_2(c) \notin \{p-1, 2p-1\}$. On the one hand, if $\nu_2(a) < \nu_2(b)$, then $\nu_2(a) = p-1$ and $\nu_2(c) = 2\nu_2(a) = 2p-2$. On the other hand, if $\nu_2(a) = \nu_2(b)$ then $\nu_2(a) \le p-2$, and $\nu_2(c) = 2\nu_2(a)+1$ is odd and less than $2p-1$.