Solutions Notes for DNY-NTCONSTRUCT

Evan Chen*

April 26, 2018

Contents

1 USAMO 2017/1 2
2 JMO 2016/2 2
3 Shortlist 2007 N2 3
4 IMO 2000/5 3
5 BAMO 2011/5 3
6 TSTST 2012/5 4
7 Shortlist 2014 N4 4
8 USA TST 2007/4 5
9 China TST 2018/2/4 5
10 EGMO 2018/2 5
11 USAMO 2006/3 6
12 USAMO 2013/5 7
13 RMM 2012/4 7
14 USAMO 2012/3 7
15 TSTST 2016/3 8
16 Shortlist 2013 N4 10
17 EGMO 2014/3 10
18 IMO 2017/6 11

*Internal use: Olympiad Training for Individual Study (OTIS). Last update April 26, 2018.

§1 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.

§2 JMO 2016/2

Prove that there exists a positive integer $n < 10^6$ such that 5^n has six consecutive zeros in its decimal representation.

One answer is $n = 20 + 2^{19} = 524308$.
First, observe that

$$\begin{aligned} 5^n &\equiv 5^{20} \pmod{5^{20}} \\ 5^n &\equiv 5^{20} \pmod{2^{20}} \end{aligned}$$

the former being immediate and the latter since $\varphi(2^{20}) = 2^{19}$. Hence $5^n \equiv 5^{20} \pmod{10^{20}}$. Moreover, we have

$$5^{20} = \frac{1}{2^{20}} \cdot 10^{20} < \frac{1}{1000^2} \cdot 10^{20} = 10^{-6} \cdot 10^{20}.$$

Thus the last 20 digits of 5^n will begin with six zeros.

Remark. Many of the first posts in the JMO 2016 discussion thread (see https://aops.com/community/c5h1230514) claimed that the problem was "super easy". In fact, the problem was solved by only about 10% of contestants.

§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 IMO 2000/5

Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

Answer: Yes.

We say that n is *Korean* if $n \mid 2^n + 1$. First, observe that $n = 9$ is Korean. Now, the problem is solved upon the following claim:

Claim. If $n > 3$ is Korean, there exists a prime p not dividing n such that np is Korean too.

Proof. I claim that one can take any primitive prime divisor p of $2^{2n} - 1$, which exists by Zsigmondy theorem. Obviously $p \neq 2$. Then:

- Since $p \nmid 2^{\varphi(n)} - 1$ it follows then that $p \nmid n$.
- Moreover, $p \mid 2^n + 1$ since $p \nmid 2^n - 1$.

Hence $np \mid 2^n + 1 \mid 2^{np} + 1$ by Chinese Theorem, since $\gcd(n, p) = 1$. $\square$

§5 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 $k=85$, $n=203$.

§6 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 $t < 2^{r+1}q < 2^{r+2}q < \cdots < 2^{r+m}q < n$. 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 $\{0, c_1\} + \{0, c_2\} + \cdots + \{0, c_m\}$ 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. $\square$

§7 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.

Suppose n is even now. Then by **Kobayashi's Theorem**, there exist infinitely many primes p dividing some number of the form

$$n^{n^r - 1} - 1.$$

for some integer r. Let $p > n$ be such a prime, with corresponding integer r. It then follows that

$$n^{n^r p} \equiv n^r \pmod{n^r p}$$

since this is clearly correct mod n^r, and also correct modulo p. If we select $k = n^r p$, we have

$$\left\lfloor \frac{n^k}{k} \right\rfloor = \frac{n^{n^r p} p - n^r}{n^r p}$$

which is odd.

§8 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 prime.

§9 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

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

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.

§10 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. $\square$

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. $\square$

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.

§11 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

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

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

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 $n \leq \frac{p-1}{2} - c$ 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 $0 \leq k \leq c$ 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.

§12 USAMO 2013/5

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

One-line spoiler: 142857.

To work out the details, there exist arbitrarily large primes p such that

$$p \mid 10^e m - n$$

for some positive integer e, say by Kobayashi theorem (or other more mundane means). In that case, the periodic decimal expansions of $\frac{m}{p}$ and $\frac{n}{p}$ are cyclic shifts of each other. Thus if one looks at $\frac{1}{p}$ the repeating block of decimals, one may take c to be that resulting integer.

Remark. The official USAMO solutions propose using the fact that 10 is a primitive root modulo 7^e for each $e \ge 1$, by Hensel lifting lemma. This argument is *incorrect*, because it breaks if either m or n are divisible by 7.

One may be tempted to resort to using large primes 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 condition necessary for this argument to work.

§13 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 $n_k = p n_{k-1}$ 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.

§14 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

$$a_k + 2a_{2k} + \dots + n a_{nk} = 0$$

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 $a_{2^k} = \frac{a_1}{2^k}$ for all k.

For $n \ge 3$ 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 $a_1 + 2a_2 + \dots + n a_n = 0$. 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 $n > 2$.

§15 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. $\square$

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

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

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

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

§16 Shortlist 2013 N4

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

The answer is no.

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

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

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

$$A_k \le B_k < 2x_{k+1} < 2 \cdot \sqrt{10^{k+1}}.$$

The idea will be that divisibility issues will force one of A_k and B_k to be too large.

We now split the proof in two cases:

- First, assume $\nu_5(x_k^2) \ge k$ for all k. Then in particular $a_1 = 5$, so all x_k are always odd. So one of A_k and B_k is divisible by 2^{k-1}. Moreover, both divisible by at least $5^{k/2}$. So for each k,
$$\min(A_k, B_k) \ge 2^{k-1} \cdot 5^{k/2}$$
which is impossible for large enough k.

- Next assume $\nu_5(x_m^2) = 2e < m$ for some m. Then since $x_{k+1}^2 \equiv x_k^2 \pmod{10^k}$, we obtain $\nu_5(x_k^2) = 2e$ for all $k > m$. Now,
$$\min(A_k, B_k) \ge 5^{k-e}$$
which again is impossible for k large enough.

§17 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 $p \mid 2(n)$.

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 $2p - 1$.

§18 IMO 2017/6

An *irreducible lattice point* is an ordered pair of integers (x, y) satisfying $\gcd(x, y) = 1$. Prove that if S is a finite set of irreducible lattice points then there exists a *homogeneous* polynomial $f(x, y)$ of degree at least 1 such that $f(x, y) = 1$ for each $(x, y) \in S$.

First solution (Dan Carmon, Israel) We prove the result by induction on $|S|$, with the base case being Bezout's Lemma ($n = 1$). For the inductive step, suppose we want to add a given pair (a_{m+1}, b_{m+1}) to $\{(a_1, \dots, a_m), (b_1, \dots, b_m)\}$. By a suitable linear transformation assume $(a_{m+1}, b_{m+1}) = (1, 0)$. (The transformation is not necessary to proceed but cleans up the presentation that follows.)

Let $g(x, y)$ be a polynomial which works on the latter set. We claim we can choose the new polynomial f of the form

$$f(x, y) = g(x, y)^M - Cx^{\deg g \cdot M - m} \prod_{i=1}^{m} (b_i x - a_i y).$$

where C and M are integer parameters we may adjust.

Since $f(a_i, b_i) = 1$ by construction we just need

$$1 = f(1, 0) = g(1, 0)^M - C \prod b_i.$$

If $\prod b_i = 0$ we are done, since $b_i = 0 \implies a_i = \pm 1$ in that case and so $g(1, 0) = \pm 1$, thus take $M = 2$. So it suffices to prove:

Claim. $\gcd(g(1, 0), b_i) = 1$ when $b_i \neq 0$.

Proof. Fix i. If $b_i = 0$ then $a_i = \pm 1$ and $g(\pm 1, 0) = \pm 1$. Otherwise know

$$1 = g(a_i, b_i) \equiv g(a_i, 0) \pmod{b_i}$$

and since the polynomial is homogeneous with $\gcd(a_i, b_i) = 1$ it follows $g(1, 0) \not\equiv 0 \pmod{b_i}$ as well. $\square$

Then take M a large even multiple of $\varphi(\prod b_i)$ and we're done.

Second solution (Lagrange) The main claim is that:

Claim. For every positive integer N, there is a homogeneous polynomial $P(x, y)$ such that $P(x, y) \equiv 1 \pmod N$ whenever $\gcd(x, y) = 1$.

(This claim is actually implied by the problem.)

Proof. For $N = p^e$ a prime take $(x^{p-1} + y^{p-1})^{\varphi(N)}$ when p is odd, and $(x^2 + xy + y^2)^{\varphi(N)}$ for $p = 2$.

Now suppose $N = q_1 q_2 \dots q_k$ where q_i are prime powers. Look at the polynomial Q_i described above for $i = 1, \dots, k$. Now

$$\frac{N}{q_i} Q_i(x, y) \equiv \frac{N}{q_i} \pmod N$$

for all x and y; so we can put together the polynomials $\frac{N}{q_i} Q_i$ by Bézout lemma. $\square$

Let $S = \{(a_i, b_i) \mid i = 1, \dots, m\}$. We have the natural homogeneous "Lagrange polynomials" $L_k(x, y) = \prod_{i \neq k} (b_i x - a_i y)$. Now let $N = \prod_k L_k(x_k, y_k)$ and take P as above. Then we can take a large power of P, and for each i subtract an appropriate multiple of $L_i(x, y)$.