DNW-EXPNT Solutions

Michael Middlezong

12 July 2024

Problem 1 (JMO 2011/1)

Obviously, $n = 1$ is a solution. Then, assume $n \geq 2$.

The expression is $(-1)^n + 1 \bmod 3$. If n is even, then it will equal $2 \bmod 3$, which is not a quadratic residue. So, n is odd.

The expression is $(-1)^n \bmod 4$. Since -1 is not a quadratic residue, n must be even. Thus, the only solution is $n = 1$.

Problem 2 (Putnam 2018 B3)

We claim that only numbers of the form $n = 2^{2^{2^r}}$ for $r \geq 0$ work.

Obviously, the first condition is true iff $n = 2^m$ for some m. Then, the second and third condition are equivalent to

$$2^n \equiv 1 \pmod{2^m - 1},$$

$$2^{n-1} \equiv 1 \pmod{2^{m-1} - 1}.$$

Looking at the first congruence, the order of 2, which is m, must divide n, so $m \mid n$. This means that $m = 2^q$ for some q.

Looking at the second congruence, the order of 2, which is $m - 1$, must divide $n - 1$, so $m - 1 \mid n - 1$. This means $n \equiv 1 \pmod{m - 1}$, or

$$2^m \equiv 1 \pmod{2^q - 1}.$$

Again, this is satisfied when $q \mid m$, so $q = 2^r$ for some r. Note that all of these steps are reversible. Therefore, the condition is necessary and sufficient.

Problem 3 (USAMO 1987/1)

First, $n = 0$ obviously works. Then, expand both sides and write it as a quadratic in n. The discriminant factors as $m(m-8)(m+1)^2$. Thus, either $m = -1$ or $m(m-8) = k^2$ for some integer k. Therefore, we have $(m-4)^2 - k^2 = 16$ and the only m that work are -1, 8, and 9.

Plugging it back in and checking the solutions gives us

$$\{(-1,-1), (8,-10), (9,-6), (9,-21)\}$$

as our set of nonzero solutions.

Problem 4 (Shortlist 2002/N1)

Taking mod 9 is enough to prove the answer is at least 4. Since $10^3+10^3+1^3+1^3 = 2002$, it is not hard to construct a working solution.

Problem 5 (Pixton)

The only solution is $(x, y) = (45, 4)$. We can manually check for $y < 6$ that $y = 4$ is the only solution. Assume $y \geq 6$. Then $9 \mid y!$, so we have $y! + 2001 \equiv 3 \pmod 9$. This means 3 divides x^2 exactly once, which is impossible.

Problem 6 (USEMO 2019/4)

We can guess that 2020 is just an arbitrary number, and try to prove that $f(n) = 1^n + 2^{n-1}+\cdots+n^1$ attains every residue mod p. Using the lemma that $1^n+2^n+\cdots+(p-1)^n = 0$ whenever $p-1 \nmid n$, we can see that $f(p(p-1)) \equiv -1 \pmod p$. Moreover, $f(cp(p-1)) \equiv -c \pmod p$ because all base-exponent combos reset every $p(p-1)$, so we are done.

Problem 8 (Brazil 2007/2)

The problem is just asking us to characterize quadratic residues mod 2^{2007}. We claim that mod 2^n, all residues which are 1 mod 8 are precisely the odd quadratic residues. It is easy to see by mods that all quadratic residues must be 1 mod 8. Next, we claim that if p and q are distinct elements of the set $\{1, 3, \ldots, 2^{n-2} - 1\}$, then $p^2 \not\equiv q^2 \pmod{2^n}$. This can be shown by analyzing $\nu_2(p^2 - q^2)$.

The above is the majority of the problem. Notice that even quadratic residues are just 4^k times an odd quadratic residue. Answer extraction is done by casework on the power of 4.

Problem 10 (Qiao Zhang)

The answer is all $n \equiv 1, 3 \pmod 8$. First, we show it is necessary. Considering mod 8, we see that if n is not 1 or 3 mod 8, then expressions of the form $3^k - n$ will never be divisible by 8.

To show it is sufficient, consider the order of 3 mod 2^m for any positive integer $m \geq 4$. By lifting the exponent, we see that the order is 2^{m-2}. Thus, the orbit of possible values of 3^a covers all residues mod 2^m which are 1 or 3 mod 8. This means that eventually, some term of the form $3^k - n$ will be divisible by 2^m, so the sequence is unbounded.

Problem 11 (Shortlist 2006/N5)

We claim there are no solutions. Suppose (x, y) is an integer solution to the equation. Then, consider a prime p dividing $\frac{x^7-1}{x-1} = y^5-1$. By the divisors of cyclotomic polynomials lemma, $p = 7$ or $p \equiv 1 \pmod 7$. This means every factor of $y^5 - 1$ is either 0 or 1 mod 7.

Consider the case where $y^5 - 1 \equiv 0 \pmod 7$. Then, we have $y \equiv 1 \pmod 7$. Since $y^4 + y^3 + y^2 + y^1 + 1 \equiv 5 \pmod 7$ is a factor dividing $y^5 - 1$, we have a contradiction.

If $y^5 - 1 \equiv 1 \pmod 7$, then we have $y \equiv 4 \pmod 7$. But then, $y - 1 \equiv 3 \pmod 7$ is a factor dividing $y^5 - 1$, so we have a contradiction.

Thus, there are no solutions.

Problem 12 (Shortlist 1998/N5)

Lemma: $m^2 \equiv -1 \pmod{p^k}$ has a solution mod p^k if and only if $p \equiv 1 \pmod 4$.

Proof. Let g be a primitive root mod p^k. Then, if $p \equiv 1 \pmod 4$, we can take $m = g^{\frac{\varphi(p^k)}{4}} = g^{\frac{p^k - p^{k-1}}{4}}$. It satisfies

$$m^2 \equiv g^{\frac{\varphi(p^k)}{2}} \equiv -1 \pmod{p^k}.$$

For the other direction, notice that m has order 4 mod p^k, so 4 divides $\varphi(p^k) = p^k - p^{k-1}$. Looking at this expression mod 4, we see that we must have $p \equiv 1 \pmod 4$. $\square$

The answer is $n = 2^a$ where $a \geq 0$.

First, let $p \mid 2^n - 1$. Then, assuming n works, there exists m such that

$$m^2 \equiv -9 \pmod p.$$

Assume $p \neq 3$. Then, we have (using our lemma)

$$\left(\frac{m}{3}\right)^2 \equiv -1 \pmod p \implies p \equiv 1 \pmod 4.$$

So, every prime dividing $2^n - 1$ must be either 3 or congruent to 1 mod 4.

We claim that if n is not of the form 2^a, then n does not work. If n is not of this form, an odd number $k > 1$ must divide n. Then, we have $2^k - 1 \mid 2^n - 1$.

Notice that $2^k - 1 \equiv 3 \pmod 4$ and $2^k - 1 \equiv 1 \pmod 3$. This implies that there exists a prime p dividing $2^k - 1$ (and thus $2^n - 1$) with $p \neq 3$ and $p \equiv 3 \pmod 4$, giving us a contradiction.

Next, we claim that all $n = 2^a$ work. Let $p \mid 2^{2^a} - 1$. Then,

$$2^{2^a} \equiv -1 \pmod p \implies 2^{2^{a+1}} \equiv 1 \pmod p.$$

This means the order of 2 mod p divides 2^{a+1}.

- If this order is 1, then $p = 1$, contradiction.
- If this order is 2, then $p = 3$.
- If this order is greater than 2, then the order is divisible by 4. Since the order divides $p - 1$, we must have $p \equiv 1 \pmod 4$.

This means every prime dividing $2^{2^a} - 1$ is either 3 or congruent to 1 mod 4. In addition, we know $2^{2^a} - 1 \equiv 0 \pmod 3$, so 3 must be one of the primes dividing $2^{2^a} - 1$.

So, let $2^{2^a} - 1 = 3p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. We claim there is an m satisfying the following congruences:

$$\begin{aligned} m^2 &\equiv -9 \pmod 3, \\ m^2 &\equiv -9 \pmod{p_1^{\alpha_1}}, \\ m^2 &\equiv -9 \pmod{p_2^{\alpha_2}}, \\ &\vdots \\ m^2 &\equiv -9 \pmod{p_k^{\alpha_k}}. \end{aligned}$$

The first congruence is equivalent to $m \equiv 0 \pmod 3$. For the other congruences, by our lemma, there exists l such that $l^2 \equiv -1 \pmod{p_i^{\alpha_i}}$. Then $m = 3l$ is the solution we want.

Therefore, we can use the Chinese Remainder Theorem to guarantee the existence of m satisfying

$$m^2 \equiv -9 \pmod{2^{2^a} - 1} \implies 2^{2^a} - 1 \mid m^2 + 9.$$

Problem 19 (IMO 1990/3)

The answer is $n = 1, 3$. We show that there are no other solutions. Since n must be odd, assume $n \geq 5$. Let p be the least prime factor of n. We have $p > 2$ since n is odd. Furthermore, $2^n + 1 \equiv 0 \implies 4^n \equiv 1 \pmod{p}$.

We claim the order of 4 mod p is 1. This is because the order must divide $\gcd n, p-1$, which must equal 1 otherwise $\gcd n, p-1$ must have smaller prime factors which also divide n, contradicting p's minimality. Thus, $4 \equiv 1 \pmod{p}$, so $p = 3$.

In order for n^2 to divide $2^n + 1$, we must have $\nu_3(n^2) = 2\nu_3(n) \leq \nu_3(2^n + 1)$. Since $3 \mid 2 + 1$, using the lifting the exponent lemma yields $\nu_3(2^n + 1) = 1 + \nu_3(n)$. We then conclude that $\nu_3(n) \leq 1$, but since 3 is the smallest prime factor of n, we must have $\nu_3(n) = 1$.

Now, we write $n = 3k$ for some k not divisible by 2 or 3. Since $n \geq 5$, we have $k > 1$ and we can let p be the smallest prime factor of k. But similarly to before, we see that $2^{6k} \equiv 1 \pmod{p}$ and thus $64 \equiv 1 \pmod{p}$. This means $p \mid 63$. Since $p \geq 5$, we must have $p = 7$.

This tells us that n^2 is divisible by 7. However, $2^n + 1 \equiv 8^k + 1 \equiv 2 \pmod{7}$, so we are done.

Problem 20 (IMO 2000/5)

Define two sequences as follows: $n_0 = 1$; p_i is (a) the smallest prime factor of $2^{n_i} + 1$ that is not a factor of n_i, or (b) if that doesn't exist, the smallest prime factor of $2^{n_i} + 1$; and $n_{i+1} = n_i p_i$.

Notice that each n_i is divisible by all of the previous ones, and that all n_i and p_i are odd.

First, we show that all n_i satisfy $n_i \mid 2^{n_i} + 1$. We proceed by induction. We can see that $n_0 = 1$ works, so assume n_i works (and all the ones before it). We want to prove $n_{i+1} \mid 2^{n_{i+1}} + 1$.

Note that if a prime p divides n_{i+1}, then $p = p_j$ for some j satisfying $0 \leq j \leq i$. This also means that p_j is a factor of $2^{n_j} + 1$. Then, by LTE, we have

$$\nu_{p_j}(2^{n_{i+1}} + 1) = \nu_{p_j}(2^{n_j} + 1) + \nu_{p_j}\left(\frac{n_{i+1}}{n_j}\right) = \nu_{p_j}(n_{i+1}) + \nu_{p_j}(2^{n_j} + 1) - \nu_{p_j}(n_j).$$

However, the strong inductive hypothesis implies $\nu_{p_j}(2^{n_j} + 1) - \nu_{p_j}(n_j) \geq 0$, so we have $\nu_{p_j}(2^{n_{i+1}} + 1) \geq \nu_{p_j}(n_{i+1})$. As this is true for all p, the inductive step is complete.

Next, we claim that eventually, the number of distinct prime factors of n_i is always one more than the number of distinct prime factors of n_{i-1}. This is equivalent to showing that eventually, there always exists a prime factor of $2^{n_i} + 1$ that is not a factor of n_i. This is essentially Zsigmondy's theorem, so we could be done here. However, I forgot that theorem existed, so here is a size argument:

Suppose, for some i, that every prime factor of $2^{n_i} + 1$ is also a factor of n_i. Then, let p be a prime factor of n_i, and pick the minimal j such that $p_j = p$. This minimality implies that $\nu_{p_j}(n_j) = 0$. We have

$$\nu_{p_j}(2^{n_i} + 1) = \nu_{p_j}(2^{n_j} + 1) + \nu_{p_j}(n_i) - \nu_{p_j}(n_j) = \nu_{p_j}(2^{n_j} + 1) + \nu_{p_j}(n_i).$$

We can raise p_j to the power of both sides to get

$$p_j^{\nu_{p_j}(2^{n_i}+1)} = p_j^{\nu_{p_j}(2^{n_j}+1)} p_j^{\nu_{p_j}(n_i)}.$$

Doing this for every prime factor p of n_i (notice that j is now a one-to-one function of p) and multiplying the resulting equations, we get

$$2^{n_i} + 1 = n_i \prod_p p^{\nu_p(2^{n_{j(p)}}+1)}.$$

For all p, we have $p^{\nu_p(2^{n_{j(p)}}+1)} \leq 2^{n_{j(p)}} + 1$. Thus,

$$2^{n_i} + 1 \leq n_i \prod_p (2^{n_{j(p)}} + 1).$$

Since j is one-to-one, every $j(p)$ is unique and in the set $\{0, 1, \ldots, i-1\}$. Therefore, we have the inequality

$$2^{n_i} + 1 \leq n_i \prod_{j=0}^{i-1} (2^{n_j} + 1).$$

Taking the log base 2 of both sides, we have

$$n_i < \log_2(2^{n_i}+1) \leq \log_2 n_i + \sum_{j=0}^{i-1} \log_2(2^{n_j}+1) < \log_2 n_i + \sum_{j=0}^{i-1}(n_j+1) = \log_2 n_i + i + \sum_{j=0}^{i-1} n_j.$$

Now, in order to achieve a bound on n_i, we notice that $p_i \geq 3$ for all i, so therefore, $n_i \geq 3^i$. It is then easy to see that $\sum_{j=0}^{i-1} n_j \leq \frac{1}{2} n_i$ for all $i \geq 1$. Then,

$$n_i < \log_2 n_i + i + \frac{1}{2} n_i \leq \log_2 n_i + \log_3 n_i + \frac{1}{2} n_i \iff n_i < 2(\log_2 n_i + \log_3 n_i).$$

This inequality obviously cannot be satisfied as n_i grows large. Thus, eventually, we must have that there exists a prime factor of $2^{n_i} + 1$ that is not a factor of n_i. Hence, there must eventually exist an n in our sequence with exactly 2000 distinct prime factors.

Problem 22 (Generalized IMO 1999/4)

We claim the solutions are $(1, p)$ for all p, $(2, 2)$, and $(3, 3)$. They can be checked to work. Furthermore, if $p = 2$, then x must be a divisor of $1^x + 1 = 2$, so $(1, 2)$ and $(2, 2)$ are the only solutions. Thus, from now on, we can assume $x > 1$ and $p \geq 3$.

We know x has a least prime factor; let that be q. Then, we have

$$(p-1)^x \equiv -1 \pmod{q}$$
$$(p-1)^{2x} \equiv 1 \pmod{q}.$$

Looking at the order of $(p-1)^2$, it must divide the GCD of $q-1$ and x. But q being the least prime factor implies that GCD is 1, so $(p-1)^2 \equiv 1 \pmod{q}$. This means $q \mid p(p-2)$.

However, $q \mid p-2$ is impossible. To see why, notice that $(p-1)^x + 1 \equiv 1 + 1 \pmod{p-2}$, so $(p-1)^x + 1 \equiv 2 \pmod{q}$. Since q is odd, this means that $(p-1)^x + 1$ is not divisible by q, contradicting the fact that x^{p-1} divides $(p-1)^x + 1$.

Thus, we must have $q = p$. Now, notice that since x must be odd, we can use lifting the exponent:

$$\nu_p((p-1)^x + 1) = 1 + \nu_p(x) \geq \nu_p(x^{p-1}) = (p-1)\nu_p(x).$$

This implies

$$\frac{1}{p-2} \geq \nu_p(x) \geq 1,$$

so $p \leq 3$.

We only need to consider the case where $p = 3$. However, the result of IMO 1990/3 tells us that $(1, 3)$ and $(3, 3)$ are the only solutions in this case, so we are done.

Problem 21 (TSTST 2018/8)

Lemma: If $a \mid b$ and a and b are odd, then $x^a + 1 \mid x^b + 1$ for all natural numbers x.

Proof. We know $\frac{b}{a}$ is odd, so

$$\frac{x^b + 1}{x^a + 1} = x^{b-a} - x^{b-2a} + x^{b-3a} - \ldots + 1.$$

□

We claim that all b such that $b + 1$ is not a power of 2 work. We will generate an infinite sequence of n's satisfying the condition, starting with $n_1 = p_1$ where p_1 is an odd prime that divides $b + 1$. The sequence will also satisfy the additional condition that n_i can be written in the form $p_1 p_2 \ldots p_i$ where the p_j's are distinct odd primes. To establish the base case, notice that since p_1 is odd, we can use lifting the exponent:

$$\nu_{p_1}(b^{p_1} + 1) = \nu_{p_1}(b + 1) + 1 \geq 2.$$

Thus, $n_1^2 \mid b^{n_1} + 1$.

Next, assume $n_i = p_1 p_2 \ldots p_i$ satisfies the condition that $n_i^2 \mid b^{n_i} + 1$. Then, let p_{i+1} be a primitive prime divisor of $b^n + 1$. Its existence is guaranteed by Zsigmondy's theorem. We claim that $p_{i+1} \neq 2$. If b is even, then that is obvious. Otherwise, $2 \mid b + 1$, so 2 would not be a primitive divisor. Thus, p_{i+1} is an odd prime distinct from any of $p_1, p_2, \ldots, p_i$.

We then claim that if $n_{i+1} = p_1 p_2 \ldots p_{i+1}$, then n_{i+1} satisfies the condition from the problem statement. By our lemma, we know that $n_i^2 = (p_1 p_2 \ldots p_i)^2 \mid b^{n_i} + 1 \mid b^{n_{i+1}} + 1$. It remains to check $p_{i+1}^2 \mid b^{n_{i+1}} + 1$. Again, we use lifting the exponent:

$$\nu_{p_{i+1}}(b^{n_{i+1}} + 1) = \nu_{p_{i+1}}(b^{n_i} + 1) + \nu_{p_{i+1}}(p_{i+1}) = \nu_{p_{i+1}}(b^{n_i} + 1) + 1 \geq 2.$$

Thus, by induction, every n in this infinite sequence works.

Finally, we prove that if $b + 1$ is a power of 2, there are finitely many solutions to $n^2 \mid b^n + 1$. Suppose $n > 1$ satisfies $n^2 \mid b^n + 1$. If n were even, then $b^n + 1$ would be either 1 or 2 mod 4, but it also must be 0 mod 4 in order to be divisible by n^2. Hence, n must be odd.

Next, let p be the least prime factor of n. We have

$$b^n \equiv -1 \implies b^{2n} \equiv 1 \pmod{p},$$

so the order of b^2 must divide $\gcd(p - 1, n)$. Since p is the least prime factor of n, this GCD must equal 1; otherwise, $\gcd(p - 1, n)$ would have a prime factor less than p which is also a factor of n, contradicting p's minimality. Thus, $b^2 \equiv 1 \pmod{p}$, or in other words, $p \mid (b - 1)(b + 1)$. We know p cannot divide $b + 1$ since $b + 1$ is a power of 2.

Thus, p must divide $b - 1$, and $b \equiv 1 \pmod{p}$. However, this means $b^n \equiv 1 \pmod{p}$, so p must be 2, which is impossible since n is odd! This concludes the proof.

Problem 26 (USEMO 2021/2)

The answer is $n \in \{1, 2, 4, 6, 8, 16, 32\}$. Let $f(n)$ be the number of divisors of $2^n - 1$, and let $d(n)$ be the number of divisors of n. Notice the function $d(n)$ is multiplicative (with relatively prime numbers). A key element of the solution is to notice that if we write $n = 2^a k$ where k is odd, then

$$2^n - 1 = (2^k - 1)(2^k + 1)(2^{2k} + 1) \cdots (2^{2^{a-1}k} + 1).$$

Furthermore, all of these factors are odd and relatively prime.

For all k, we have

$$f(2k) = d(2^{2k} - 1) = d(2^k - 1)d(2^k + 1) = f(k)d(2^k + 1).$$

Therefore, $f(2k) \geq 2f(k)$ with equality iff $2^k + 1$ is prime. This means that if $f(k) = k$ but $2^k + 1$ is not prime, multiplying k by a power of 2 is guaranteed to fail. Along with the fact that $2^{2^5} + 1$ is not prime (look at Fermat primes), this is enough to show that the only powers of 2 satisfying $f(n) = n$ are 1, 2, 4, 8, 16, and 32.

If n is not a power of 2, then write $n = 2^a k$ where k is odd and $k \geq 3$. At this point, we claim that n must be even, so we can make this useful. If n is odd and $f(n) = n$, then this implies $2^n - 1$ is a perfect square. However, looking mod 4, this is only true when $n = 1$. Thus, n must be even and $a \geq 1$.

Then, looking at the ν_2 of

$$f(2^a k) = f(k)d(2^k + 1)d(2^{2^k} + 1) \cdots d(2^{2^{a-1}k} + 1),$$

we see that $2^k + 1$ must be a perfect square. Mihailescu's theorem tells us that the only possible solution to this is $k = 3$, but here is another way to see it.

Let $2^k + 1 = m^2$. Then, we have $2^k = (m - 1)(m + 1)$. Thus, $m - 1$ and $m + 1$ must both be powers of 2, but the only powers of 2 that differ by 2 are $2^1 = 2$ and $2^2 = 4$, so we must have $k = 3$.

Anyways, we can manually verify that $n = 6$ does work but $n = 12$ does not. We turn again to the fact that $f(2k) \geq 2f(k)$ with equality iff $2^k + 1$ is prime. Unfortunately, $2^6 + 1$ is not prime, so we are done.