Lifting The Exponent Lemma (LTE)

Version 6 - Amir Hossein Parvardi

April 7, 2011

Lifting The Exponent Lemma是求解指数丢番图方程(不定方程)的有效方法。它在奥林匹克民间传说中非常有名（例如，参见[3]），尽管其起源很难追溯。在数学上，它是数论中经典Hensel引理（见[2]）的近亲（在证明的陈述和观点中）。在本文中，我们分析了这种方法并介绍了它的一些应用。

在涉及指数方程的许多问题中，我们可以使用Lifting The Exponent Lemma（这是一个长名称，我们称之为LTE！）,特别是我们可以找到某些质因子的时候。有时LTE引理甚至能秒杀一道题。这个引理显示了如何找到素数p的最大幂 —— 通常⩾3 —— a^n ±b^n型——本文中定理和引理的证明没有任何复杂难理解之处，所有这些都使用了初等数学。理解定理的用法及其含义对于你来说比记住它的详细证明更重要。

我要感谢Fedja，darijgrinberg（Darij Grinberg），makar和ZetaX（Daniel）对这篇文章的帮助。我特别感谢JBL（Joel）和Fedja对TeX的帮助。

1 定义和符号

对于两个整数a和b，我们说a可被b整除并写入b | a且仅当存在某个整数q时a =qb。

我们将 $v_p(x)$ 定义为素数p除以x的最大幂; 特别是，当 $v_p(x) = \alpha$ ， $p^\alpha \mid x$ 但是 $p^{\alpha+1} \nmid x$. 我们也会写成 $p^\alpha \| x$, 当且仅当 if $v_p(x) = \alpha$. 所以我们有 $v_p(xy) = v_p(x) + v_p(y)$ 和 $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

例子. 除以 63 的3的最大幂 是 3^2. 因为$3^2 = 9 \mid 63$ 但是 $3^3 = 27 \nmid 63$.特别的, $3^2 \| 63$ 或 $v_3(63) = 2$.

例子. 显然，我们看到如果p和q是两个不同的素数，那么$v_p(p^\alpha q^\beta) = \alpha$, or $p^\alpha \| p^\alpha q^\beta$.

注意. 对于所有素数p $v_p(0) = \infty$.

2 两个重要且有用的引理

引理**1.**令x和y为（不必为正）整数，并使n为正整数。 给定任意素数p（p = **2**是特别的情况），使得gcd（n，p）= **1**，p | x-y并且x和y都不能被p整除（即，p∤x和p∤y）。 我们有

$$v_p(x^n - y^n) = v_p(x - y).$$

证明. 我们有

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}).$$

现在，如果我们证明了 $p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}$, 那么我们就做完了. 表明这一点，我们使用假设p | x - y。 所以我们有x - y≡0（mod p），或x≡y（mod p）。 从而

$$\begin{aligned} x^{n-1} &+ x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1} \\ &\equiv x^{n-1} + x^{n-2} \cdot x + x^{n-3} \cdot x^2 + \cdots + x \cdot x^{n-2} + x^{n-1} \\ &\equiv nx^{n-1} \\ &\not\equiv 0 \pmod{p}. \end{aligned}$$

这样就完成了证明。 □

引理**2.**设x和y为（不必为正）整数，令n为奇数正整数。 给定任意素数p（p = **2**是特别的情况），使得gcd（n，p）= **1**，p | x + y并且x和y都不能被p整除，我们有

$$v_p(x^n + y^n) = v_p(x + y).$$

证明： 由于x和y可以是负数，因此使用引理1得到

$$v_p(x^n - (-y)^n) = v_p(x - (-y)) \implies v_p(x^n + y^n) = v_p(x + y).$$

注意，由于n是奇数正整数，我们可以用 $(-y)^n$ 替换 $-y^n$. □

3 Lifting The Exponent Lemma (LTE)

定理**1**（**LTE**的第一种形式）。

设x和y为（不必为正）整数，令n为正整数，令p为奇数素数，使得p | x-y并且x和y都不能被p整除（即，p∤x和p∤y）。 我们有

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

证明：我们对$v_p(n)$使用归纳法.首先，让我们证明以下:

$$v_p(x^p - y^p) = v_p(x - y) + 1. \tag{1}$$

为了证明这个，我们要证明以下

$$p \mid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{2}$$

和

$$p^2 \nmid x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}. \tag{3}$$

对于 **(2)**, 我们注意到

$$x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod p.$$

现在，令 $y = x + kp$, k是整数.对于一个整数$1 \le t < p$ 我们有 $y^t x^{p-1-t} \equiv (x + kp)^t x^{p-1-t}$

$$\begin{aligned}
&\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1}) + \frac{t(t-1)}{2}(kp)^2(x^{t-2}) + \cdots\right) \\
&\equiv x^{p-1-t}\left(x^t + t(kp)(x^{t-1})\right) \\
&\equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}.
\end{aligned}$$

这意味着

$$y^t x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2} \pmod{p^2}, \quad t = 1, 2, 3, 4, \ldots, p-1.$$

由此可得

$$\begin{aligned}
&x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \\
&\quad \equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \cdots + (x^{p-1} + (p-1)kpx^{p-2}) \\
&\quad \equiv px^{p-1} + (1 + 2 + \cdots + p - 1)kpx^{p-2} \\
&\quad \equiv px^{p-1} + \left(\frac{p(p-1)}{2}\right)kpx^{p-2} \\
&\quad \equiv px^{p-1} + \left(\frac{p-1}{2}\right)kp^2x^{p-1} \\
&\quad \equiv px^{p-1} \not\equiv 0 \pmod{p^2}.
\end{aligned}$$

所以我们证明了（3）并且（1）的证明是完整的。 现在让我们回到我们的问题。 我们想证明这一点

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$

假设 $n = p^\alpha b$ 其中 $\gcd(p, b) = 1$. 然后

$$\begin{aligned}
v_p(x^n - y^n) &= v_p((x^{p^\alpha})^b - (y^{p^\alpha})^b) \\
&= v_p(x^{p^\alpha} - y^{p^\alpha}) = v_p((x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p) \\
&= v_p(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}) + 1 = v_p((x^{p^{\alpha-2}})^p - (y^{p^{\alpha-2}})^p) + 1 \\
&= v_p(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}) + 2 \\
&\;\;\vdots \\
&= v_p((x^{p^1})^1 - (y^{p^1})^1) + \alpha - 1 = v_p(x-y) + \alpha \\
&= v_p(x-y) + v_p(n).
\end{aligned}$$

注意到我们使用了当p | x-y，则p | xk -yk，因为我们有x - y | xk -yk表示所有正整数k。 证明完成了。 □

定理**2**（**LTE**的第二种形式）。 令x，y为两个整数，**n**为奇数正整数，p为奇数素数，使得p | x + y并且x和y都不能被p整除。 我们有

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

证明。 使用定理*1*这是显而易见的。请参阅我们在引理*2*的证明中使用的技巧。

□

4 $p = 2$的情况呢?

问题：为什么我们假设p是奇素数，即 $p \neq 2$? 为什么我们不能在我们的证明中假设p = 2?

提示 **.**请你注意到$\frac{p-1}{2}$ 是整数仅当 $p > 2$.

定理**3**（对于情况p = **2**的**LTE**）。 设x和y为两个奇数整数，使得**4** | x - y。然后

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

证明。 我们证明了对于任何素数*p*，*gcd*（*p*，*n*）= *1*，*p* | *x - y*并且*x*和*y*都不能被*p*整除，我们有

$$v_p(x^n - y^n) = v_p(x - y)$$

因此，它可以表明这一点：

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n.$$

因式分解得到：

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y)$$

现在，因为x≡y≡±1（mod 4），我们对所有正整数k都有$x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$ 而且 $x^{2^k} + y^{2^k} \equiv 2 \pmod 4), k = 1, 2, 3, \ldots$. 此外，由于x和y是奇数而4 | x - y，我们有x +y≡2（mod 4）。这意味着上述的所有因子(除了 $x - y$)的2的幂为1.

□

定理**4.**令x和y为两个奇数整数，令**n**为偶数正整数。 然后

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

证明。 我们知道奇数的平方是4k + 1的形式。 所以对于奇数x和y我们有 $4 \mid x^2 - y^2$. 现在让m为奇整数，k为正整数，使得$n = m \cdot 2^k$. 然后

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{m\cdot 2^k} - y^{m\cdot 2^k}) \\ &= v_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) \\ &\vdots \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x-y) + v_2(x+y) + v_2(n) - 1. \end{aligned}$$

□

5 摘要

设p是素数，让x和y为两个（不是必需的正数）整数，它们不能被p整除。 然后：

a) 对于一个正整数n

- 如果$p \neq 2$ 且 $p \mid x - y$, 那么
$$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$
- 如果 $p = 2$ 且$4 \mid x - y$, 那么
$$v_2(x^n - y^n) = v_2(x-y) + v_2(n).$$
- 如果$p = 2$, n is 偶数, 且$2 \mid x - y$, 那么
$$v_2(x^n - y^n) = v_2(x-y) + v_2(x+y) + v_2(n) - 1.$$

b) 对于奇数正整数n，如果p | x + y，那么

$$v_p(x^n + y^n) = v_p(x+y) + v_p(n).$$

c) 对于具有gcd（p，n）= 1的正整数n，如果p | x - y，有

$$v_p(x^n - y^n) = v_p(x-y).$$

如果n是奇数，则gcd（p，n）= 1，并且p | x + y，有

$$v_p(x^n + y^n) = v_p(x+y).$$

注意。使用LTE时最常见的错误是当你不检查p | x ± y的条件，所以要记得检查它。 否则你的解决方案将完全错误.

6 一些问题及答案详解

Problem 1 (Russia 1996)**.** *Find all positive integers n for which there exist positive integers x, y and k such that $\gcd(x, y) = 1, k > 1$ and $3^n = x^k + y^k$.*

Solution. k should be an odd integer (otherwise, if k is even, then x^k and y^k are perfect squares, and it is well known that for integers a, b we have $3 \mid a^2 + b^2$ if and only if $3 \mid a$ and $3 \mid b$, which is in contradiction with $\gcd(x, y) = 1$.). Suppose that there exists a prime p such that $p \mid x + y$. This prime should be odd. So $v_p(3^n) = v_p(x^k + y^k)$, and using **Theorem 2** we have $v_p(3^n) = v_p(x^k + y^k) = v_p(k) + v_p(x + y)$. But $p \mid x + y$ means that $v_p(x + y) \geq 1 > 0$ and so $v_p(3^n) = v_p(k) + v_p(x + y) > 0$ and so $p \mid 3^n$. Thus $p = 3$. This means $x + y = 3^m$ for some positive integer m. Note that $n = v_3(k) + m$. There are two cases:

- $m > 1$. We can prove by induction that $3^a \geq a + 2$ for all integers $a \geq 1$, and so we have $v_3(k) \leq k - 2$ (why?). Let $M = \max(x, y)$. Since $x + y = 3^m \geq 9$, we have $M \geq 5$. Then

$$\begin{aligned} x^k + y^k \geq M^k = \underbrace{M}_{\geq \frac{x+y}{2} = \frac{1}{2}\cdot 3^m} \cdot \underbrace{M^{k-1}}_{\geq 5^{k-1}} &> \frac{1}{2} 3^m \cdot 5^{k-1} \\ &> 3^m \cdot 5^{k-2} \geq 3^{m+k-2} \geq 3^{m+v_3(k)} = 3^n \end{aligned}$$

  which is a contradiction.

- $m = 1$. Then $x + y = 3$, so $x = 1, y = 2$ (or $x = 2, y = 1$). Thus $3^{1+v_3(k)} = 1 + 2^k$. But note that $3^{v_3(k)} \mid k$ so $3^{v_3(k)} \leq k$. Thus

$$1 + 2^k = 3^{v_3(k)+1} = 3 \cdot \underbrace{3^{v_3(k)}}_{\leq k} \leq 3k \implies 2^k + 1 \leq 3k.$$

  And one can check that the only odd value of $k > 1$ that satisfies the above inequality is $k = 3$. So $(x, y, n, k) = (1, 2, 2, 3), (2, 1, 2, 3)$ in this case.

Thus, the final answer is $n = 2$.

Problem 2 (Balkan 1993)**.** *Let p be a prime number and $m > 1$ be a positive integer. Show that if for some positive integers $x > 1, y > 1$ we have*

$$\frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m,$$

then $m = p$.

Solution. One can prove by induction on p that $\frac{x^p+y^p}{2} \geq \left(\frac{x+y}{2}\right)^p$ for all positive integers p. Now since $\frac{x^p+y^p}{2} = \left(\frac{x+y}{2}\right)^m$, we should have $m \geq p$. Let $d = \gcd(x, y)$, so there exist positive integers x_1, y_1 with $\gcd(x_1, y_1) = 1$ such that $x = dx_1$, $y = dy_1$ and $2^{m-1}(x_1^p + y_1^p) = d^{m-p}(x_1 + y_1)^m$. There are two cases:

Assume that p is odd. Take any prime divisor q of x_1+y_1 and let $v = v_q(x_1+y_1)$. If q is odd, we see that $v_q(x_1^p+y_1^p) = v+v_q(p)$ and $v_q(d^{m-p}(x_1+y_1)^m) \geq mv$ (because q may also be a factor of d). Thus $m \leq 2$ and $p \leq 2$, giving an immediate contradiction. If $q = 2$, then $m-1+v \geq mv$, so $v \leq 1$ and $x_1+y_1 = 2$, i.e., $x = y$, which immediately implies $m = p$.

Assume that $p = 2$. We notice that for $x+y \geq 4$ we have $\frac{x^2+y^2}{2} < 2\left(\frac{x+y}{2}\right)^2 \leq \left(\frac{x+y}{2}\right)^3$, so $m = 2$. It remains to check that the remaining cases $(x, y) = (1, 2), (2, 1)$ are impossible.

Problem 3. *Find all positive integers a, b that are greater than 1 and satisfy*

$$b^a | a^b - 1.$$

Solution. Let p be the least prime divisor of b. Let m be the least positive integer for which $p|a^m - 1$. Then $m|b$ and $m \mid p-1$, so any prime divisor of m divides b and is less than p. Thus, not to run into a contradiction, we must have $m = 1$. Now, if p is odd, we have $av_p(b) \leq v_p(a-1) + v_p(b)$, so $a-1 \leq (a-1)v_p(b) \leq v_p(a-1)$, which is impossible. Thus $p = 2$, b is even, a is odd and $av_2(b) \leq v_2(a-1)+v_2(a+1)+v_2(b)-1$ whence $a \leq (a-1)v_2(b)+1 \leq v_2(a-1)+v_2(a+1)$, which is possible only if $a = 3$, $v_2(b) = 1$. Put $b = 2B$ with odd B and rewrite the condition as $2^3B^3 \mid 3^{2B} - 1$. Let q be the least prime divisor of B (now, surely, odd). Let n be the least positive integer such that $q \mid 3^n - 1$. Then $n \mid 2B$ and $n \mid q-1$ whence n must be 1 or 2 (or B has a smaller prime divisor), so $q \mid 3-1 = 2$ or $q \mid 3^2 - 1 = 8$, which is impossible. Thus $B = 1$ and $b = 2$.

Problem 4. *Find all positive integer solutions of the equation $x^{2009}+y^{2009} = 7^z$*

Solution. Factor 2009. We have $2009 = 7^2 \cdot 41$. Since $x+y \mid x^{2009}+y^{2009}$ and $x+y > 1$, we must have $7 \mid x+y$. Removing the highest possible power of 7 from x, y, we get $v_7(x^{2009}+y^{2009}) = v_7(x+y)+v_7(2009) = v_7(x+y)+2$, so $x^{2009}+y^{2009} = 49 \cdot k \cdot (x+y)$ where $7 \nmid k$. But we have $x^{2009}+y^{2009} = 7^z$, which means the only prime factor of $x^{2009}+y^{2009}$ is 7, so $k = 1$). Thus $x^{2009}+y^{2009} = 49(x+y)$. But in this equation the left hand side is much larger than the right hand one if $\max(x, y) > 1$, and, clearly, $(x, y) = (1, 1)$ is not a solution. Thus the given equation does not have any solutions in the set of positive integers.

7 问题挑战

1. Let k be a positive integer. Find all positive integers n such that $3^k \mid 2^n - 1$.

2 (UNESCO Competition 1995)**.** Let a, n be two positive integers and let p be an odd prime number such that

$$a^p \equiv 1 \pmod{p^n}.$$

Prove that

$$a \equiv 1 \pmod{p^{n-1}}.$$

3 (Iran Second Round 2008)**.** Show that the only positive integer value of a for which $4(a^n + 1)$ is a perfect cube for all positive integers n, is 1.

4. Let $k > 1$ be an integer. Show that there exists infinitely many positive integers n such that

$$n | 1^n + 2^n + 3^n + \cdots + k^n.$$

5 (Ireland 1996)**.** Let p be a prime number, and a and n positive integers. Prove that if

$$2^p + 3^p = a^n$$

then $n = 1$.

6 (Russia 1996)**.** Let x, y, p, n, k be positive integers such that n is odd and p is an odd prime. Prove that if $x^n + y^n = p^k$, then n is a power of p.

7. Find the sum of all the divisors d of $N = 19^{88} - 1$ which are of the form $d = 2^a 3^b$ with $a, b \in \mathbb{N}$.

8. Let p be a prime number. Solve the equation $a^p - 1 = p^k$ in the set of positive integers.

9. Find all solutions of the equation

$$(n-1)! + 1 = n^m$$

in positive integers.

10 (Bulgaria 1997)**.** For some positive integer n, the number $3^n - 2^n$ is a perfect power of a prime. Prove that n is a prime.

11. Let m, n, b be three positive integers with $m \neq n$ and $b > 1$. Show that if prime divisors of the numbers $b^n - 1$ and $b^m - 1$ be the same, then $b + 1$ is a perfect power of 2.

12 (IMO ShortList 1991)**.** Find the highest degree k of 1991 for which 1991^k divides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

13. Prove that the number $a^{a-1} - 1$ is never square-free for all integers $a > 2$.

14 (Czech Slovakia 1996)**.** Find all positive integers x, y such that $p^x - y^p = 1$, where p is a prime.

15. Let x and y be two positive rational numbers such that for infinitely many positive integers n, the number $x^n - y^n$ is a positive integer. Show that x and y are both positive integers.

16 (IMO 2000)**.** Does there exist a positive integer n such that n has exactly 2000 prime divisors and n divides $2^n + 1$?

17 (China Western Mathematical Olympiad 2010)**.** Suppose that m and k are non-negative integers, and $p = 2^{2^m} + 1$ is a prime number. Prove that

- $2^{2^{m+1}p^k} \equiv 1 \pmod{p^{k+1}}$;
- $2^{m+1}p^k$ is the smallest positive integer n satisfying the congruence equation $2^n \equiv 1 \pmod{p^{k+1}}$.

18. Let $p \geq 5$ be a prime. Find the maximum value of positive integer k such that

$$p^k | (p-2)^{2(p-1)} - (p-4)^{p-1}.$$

19. Let a, b be distinct real numbers such that the numbers

$$a - b,\ a^2 - b^2,\ a^3 - b^3, \dots$$

are all integers. Prove that a, b are both integers.

20 (MOSP 2001)**.** Find all quadruples of positive integers (x, r, p, n) such that p is a prime number, $n, r > 1$ and $x^r - 1 = p^n$.

21 (China TST 2009)**.** Let $a > b > 1$ be positive integers and b be an odd number, let n be a positive integer. If $b^n \mid a^n - 1$, then show that $a^b > \frac{3^n}{n}$.

22 (Romanian Junior Balkan TST 2008)**.** Let p be a prime number, $p \neq 3$, and integers a, b such that $p \mid a + b$ and $p^2 \mid a^3 + b^3$. Prove that $p^2 \mid a + b$ or $p^3 \mid a^3 + b^3$.

23. Let m and n be positive integers. Prove that for each odd positive integer b there are infinitely many primes p such that $p^n \equiv 1 \pmod{b^m}$ implies $b^{m-1} \mid n$.

24 (IMO 1990)**.** Determine all integers $n > 1$ such that

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

is an integer.

25. Find all positive integers n such that

$$\frac{2^{n-1} + 1}{n}.$$

is an integer.

26. Find all primes p, q such that $\dfrac{(5^p - 2^p)(5^q - 2^q)}{pq}$ is an integer.

27. For some natural number n let a be the greatest natural number for which $5^n - 3^n$ is divisible by 2^a. Also let b be the greatest natural number such that $2^b \le n$. Prove that $a \le b + 3$.

28. Determine all sets of non-negative integers x, y and z which satisfy the equation

$$2^x + 3^y = z^2.$$

29 (IMO ShortList 2007)**.** Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that for every $m, n \in \mathbb{N}$ and every prime p, the number $f(m+n)$ is divisible by p if and only if $f(m) + f(n)$ is divisible by p.

30 (Romania TST 1994)**.** Let n be an odd positive integer. Prove that $((n-1)^n + 1)^2$ divides $n(n-1)^{(n-1)^n+1} + n$.

31. Find all positive integers n such that $3^n - 1$ is divisible by 2^n.

32 (Romania TST 2009)**.** Let $a, n \ge 2$ be two integers, which have the following property: there exists an integer $k \ge 2$, such that n divides $(a-1)^k$. Prove that n also divides $a^{n-1} + a^{n-2} + \cdots + a + 1$.

33. Find all the positive integers a such that $\frac{5^a+1}{3^a}$ is a positive integer.

8 选定问题的提示和解答

1. Answer: $n = 2 \cdot 3^{k-1}s$ for some $s \in \mathbb{N}$.

2. Show that $v_p(a-1) = v_p(a^p - 1) - 1 \geq n - 1$.

3. If $a > 1$, $a^2 + 1$ is not a power of 2 (because it is > 2 and either 1 or 2 modulo 4). Choose some odd prime $p | a^2 + 1$. Now, take some $n = 2m$ with odd m and notice that $v_p(4(a^n + 1)) = v_p(a^2 + 1) + v_p(m)$ but $v_p(m)$ can be anything we want modulo 3.

5. $2^p + 3^p$ is not a square, and use the fact that $v_5(2^p + 3^p) = 1 + v_5(p) \leq 2$.

8. Consider two cases : $p = 2$ and p is an odd prime. The latter does not give any solutions.

9. $(n, m) = (2, 1)$ is a solution. In other cases, show that n is an odd prime and m is even. The other solution is $(n, m) = (5, 2)$.

12. Answer: $\max(k) = 1991$.

13. Take any odd prime p such that $p \mid a - 1$. It's clear that $p^2 \mid a^{a-1} - 1$.

14. Answer: $(p, x, y) = (2, 1, 1), (3, 2, 1)$.

18. Let $p - 1 = 2^s m$ and show that $v_p(2^{s-1}m) = 0$. The maximum of k is 1.

19. Try to prove Problem **15** first.

20. Show that $p = 2$ and r is an even positive integer.

22. If $p \mid a, p \mid b$, then $p^3 \mid a^3 + b^3$. Otherwise LTE applies and $v_p(a + b) = v_p(a^3 + b^3) \geq 2$.

24. The answer is $n = 1$ or $n = 3$.

26. Answer: $(p, q) = (3, 3), (3, 13)$.

27. If n is odd, then $a = 1$. If n is even, then $a = v_2(5^n - 3^n) = v_2(5 - 3) + v_2(5 + 3) + v_2(n) - 1 = 3 + v_2(n)$. But, clearly, $b \geq v_2(n)$.

30. $n \mid (n-1)^n + 1$, so for every $p \mid (n-1)^n + 1$, we have

$$\begin{aligned} v_p((n-1)^{(n-1)^n+1} + 1) &= v_p((n-1)^n + 1) + v_p\left(\frac{(n-1)^{n+1} + 1}{n}\right) \\ &= 2v_p((n-1)^n + 1) - v_p(n) \end{aligned}$$

which completes the proof.

31. $n \leq v_2(3^n - 1) \leq 3 + v_2(n)$, so $n \leq 4$.

33. a must be odd (otherwise the numerator is $2 \mod 3$). Then $a \leq v_3(5^a + 1) = 1 + v_3(a)$ giving $a = 1$ as the only solution.

参考：

[1] Sepehr Ghazi Nezami, **Leme Do Khat** (in English: Lifting The Exponent Lemma) published on October 2009.

[2] Kurt Hensel, **Hensel's lemma**, WikiPedia.

[3] Santiago Cuellar, Jose Alejandro Samper, *A nice and tricky lemma (lifting the exponent)*, Mathematical Reflections **3** - 2007.

[4] Amir Hossein Parvardi, Fedja et al., AoPS **topic** #393335, *Lifting The Exponent Lemma (Containing PDF file).*

[5] Orlando Doehring et al., AoPS **topic** #214717, *Number* $\bmod (f(m+n),p)=0$ *iff* $\bmod (f(m)+f(n),p)=0$.

[6] Fang-jh et al., AoPS **topic** #268964, *China TST, Quiz 6, Problem 1.*

[7] Valentin Vornicu et al., AoPS **topic** #57607, *exactly 2000 prime divisors (IMO 2000 P5).*

[8] Orlando Doehring et al., AoPS **topic** #220915, *Highest degree for 3-layer power tower.*

[9] Sorush Oraki, Johan Gunardi, AoPS **topic** #368210, *Prove that* $a=1$ *if* $4(a^n+1)$ *is a cube for all* n.