数学竞赛中的黑科技-系列 01

指数提升定理

北京一零一中学数学竞赛小组 翻译

一 概述

指数提升定理是解决有关指数的不定方程的有力工具，它在许多难度较高的数学竞赛问题中往往有着出奇制胜的作用.在这篇文章中我们将重点讲解指数提升定理的证明方法和简单运用.

指数提升定理的主要用途是探究质数 p（一般地，$p \geq 3$）整除$a^n \pm b^n$的能力，这里 a 和 b 都是正整数.对于中学生来说证明过程可能会有一点复杂，但编者认为，比起记住本文中所证明的一些结论，看懂并学会论证的过程更能够提升考生的数学能力.

注意：本篇的所有知识点均不可以直接在高联中直接使用，使用时须给出完整证明；若在高联级别以上的考试中使用，须注明定理的名称及完整叙述.

二 定义及标记

我们定义这样的一个函数$v_p(x)$：它表示正整数 x 能够被 p 整除的最大幂次，这里 p 是一个质数.用数学语言来讲，设$\alpha = v_p(x)$，则有$p^{\alpha}||x$成立（即$p^{\alpha}|x$但$p^{\alpha+1} \nmid x$）

三 两个重要的引理

引理一 设$x, y \in \mathbb{Z}$且$x \neq y$，$n \in \mathbb{N}^*$.若对于质数 p（特殊地，可以使$p = 2$）使得 n 与 p 互质，$p|x-y$且$p \nmid x$，则有

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

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

下面只需证$p \nmid x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}$即可.又

$$\begin{aligned} & x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1} \\ \equiv\ & x^{n-1} + x^{n-2}x + x^{n-3}x^2 + \cdots + x^{n-1} \\ \equiv\ & nx^{n-1} \\ \not\equiv\ & 0 (mod\ p) \end{aligned}$$

引理一证毕.

引理二 设$x, y \in \mathbb{Z}$，n 为正偶数.若对于质数 p（特殊地，可以使$p = 2$）使得 n 与 p 互质，$p|x+y$且$p \nmid x$，则有

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

证明 利用引理一，我们有

$$v_p\big(x^n - (-y^n)\big) = v_p\big(x - (-y)\big) \Longrightarrow v_p(x^n + y^n) = v_p(x + y)$$

这里利用了 n 是偶数的性质.

四 指数提升定理

定理一（指数提升定理的第一形式）设$x, y \in \mathbb{Z}$且$x \neq y$，$n \in \mathbb{N}^*$.若对于奇质数 p 使得$p|x-y$且$p \nmid x$，则有

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

证明 利用数学归纳法.首先证明：

$$v_p(x^p - y^p) = v_p(x - y) + 1 \qquad ①$$

只需证

$$p|x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \qquad ②$$

以及

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

对于②，我们有

$$x^{p-1}+x^{p-2}y+\cdots+xy^{p-2}+y^{p-1}\equiv \mathrm{p}x^{p-1}\equiv 0(mod\ p)$$

下面设$\mathrm{y}=\mathrm{x}+\mathrm{kp}$，其中$\mathrm{k}\in\mathbb{Z}$.对于整数$1\le \mathrm{t}<\mathrm{p}$我们有

$$y^t x^{p-1-t}\equiv (x+kp)^t x^{p-1-t}$$

$$\equiv x^{p-1-t}\left(x^t+t(kp)(x^{t-1})+\frac{t(t-1)}{2}(kp)^2(x^{t-2})+\cdots\right)$$

$$\equiv x^{p-1-t}\left(x^t+t(kp)(x^{t-1})\right)$$

$$\equiv x^{p-1}+tkpx^{p-2}(mod\ p^2)$$

这就意味着

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

根据这一点，我们可以推知

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

$$\equiv x^{p-1}+(x^{p-1}+kpx^{p-2})+(x^{p-1}+2kpx^{p-2})+\cdots+(x^{p-1}+(p-1)kpx^{p-2})$$

$$\equiv px^{p-1}+(1+2+\cdots+p-1)kpx^{p-2}$$

$$\equiv px^{p-1}+\left(\frac{p(p-1)}{2}\right)kpx^{p-2}$$

$$\equiv px^{p-1}+\left(\frac{p-1}{2}\right)kp^2x^{p-2}$$

$$\equiv px^{p-1}\not\equiv 0(mod\ p^2)$$

以上我们完成了③以及①的证明.现在回到我们原本的问题.

假设$\mathrm{n}=p^{\alpha}b$，其中$\mathrm{p}\nmid\mathrm{b}$.则

$$v_p(x^n-y^n)=v_p\left(\left(x^{p^{\alpha}}\right)^b-\left(y^{p^{\alpha}}\right)^b\right)$$

$$=v_p\left(x^{p^{\alpha}}-y^{p^{\alpha}}\right)=v_p\left(\left(x^{p^{\alpha-1}}\right)^p-\left(y^{p^{\alpha-1}}\right)^p\right)$$

$$=v_p\left(x^{p^{\alpha-1}}-y^{p^{\alpha-1}}\right)+1=v_p\left(\left(x^{p^{\alpha-2}}\right)^p-\left(y^{p^{\alpha-2}}\right)^p\right)+1$$

$$=v_p\left(x^{p^{\alpha-2}}-y^{p^{\alpha-2}}\right)+2=\cdots=v_p(x-y)+\alpha$$

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

至此，证明完毕.

定理二（指数提升定理的第二形式）设$\mathrm{x},\ \mathrm{y}\in\mathbb{Z}$且$\mathrm{x}\neq\mathrm{y}$，n 为正奇数.若对于奇质数 p 使得$\mathrm{p}|\mathrm{x}+\mathrm{y}$且$\mathrm{p}\nmid\mathrm{x}$，则有

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

利用定理一，可以轻松地证明定理二.这里不再赘述.

四 当$\mathbf{p}=2$时的情况

定理三（指数提升定理当 p=2 时的形式）设两个不同的奇数 x，y 满足$4|\mathrm{x}-\mathrm{y}$.则

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

证明 根据引理一，设$\mathrm{x},\ \mathrm{y}\in\mathbb{Z}$且$\mathrm{x}\neq\mathrm{y}$，$\mathrm{n}\in\mathbb{N}^*$.若对于质数 p（特殊地，可以使$\mathrm{p}=2$）使得 n 与 p 互质，$\mathrm{p}|\mathrm{x}-\mathrm{y}$且$\mathrm{p}\nmid\mathrm{x}$，则有

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

因此只需证：

$$v_2\left(x^{2^n}-y^{2^n}\right)=v_2(x-y)+n$$

根据因式分解，可知

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

因为$x\equiv y\equiv\pm1(mod\ 4)$则我们有$x^{2^k}\equiv y^{2^k}\equiv1(mod\ 4)$对任何$k\in\mathbb{N}^*$均成立，则$x^{2^k}+y^{2^k}\equiv2(mod\ 4)$.以及，由于$4|x-y$，则有$x+y\equiv2(mod\ 4)$由上可知，在这些因式中除了$x-y$以外都被 2 恰整除，因而要证明的结论成立.

定理四 设x，y是两个不同的奇数，n 是个正偶数，则

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

证明 我们知道奇数的平方数都是$4k+1$的形式.因而$4|x^2-y^2$.现在设 m 为奇数、$k\in\mathbb{N}^*$使得$n=m\cdot2^k$，则

$$v_2(x^n-y^n)=v_2\left(x^{m\cdot2^k}-y^{m\cdot2^k}\right)$$

$$=v_2\left((x^2)^{2^{k-1}}-(y^2)^{2^{k-1}}\right)=\cdots=v_2(x^2-y^2)+k-1$$

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

五 例题

例（第十五届女子数学奥林匹克）设整数 m，n 互素，且都大于 1.

证明：存在正整数 a，b，c，满足$m^a=1+n^bc$，且 c 与 n 互素.

证：移项，$m^a-1=n^bc$.我们设$n=\prod_{i=1}^{s}p_i^{\alpha_i}$，其中$p_i$是质数.

观察到，只需取到适当的 a 和 b 使之满足$v_{p_i}(m^a-1)=b\alpha_i$，那么满足条件的 c 就一定存在.

考虑使用指数提升定理来解决问题，然而我们并不能保证该定理的使用条件$p_i|m-1$成立.怎么办呢？

联想到费马小定理：$m^{p_i-1}\equiv1(mod\ p_i)$，可以为我们解决整除的问题.于是我们换元：令$m_0=m^{\prod_{i=1}^{s}(p_i-1)}$，则可以保证对任意$p_i$，都有$p_i|m_0-1$成立.

设$m_0-1=k\prod_{i=1}^{s}p_i^{\beta_i}$，k 与任何$p_i$都互素.我们只需找到合适的正整数 b、t，使得$v_{p_i}(m_0^t-1)=b\alpha_i$即可.

事实上$v_{p_i}(m_0^t-1)=v_{p_i}(m_0-1)+v_{p_i}(t)=\beta_i+v_{p_i}(t)$

故只需令 b 取足够大的正整数，$t=\prod_{i=1}^{s}p_i^{b\alpha_i-\beta_i}$，即可满足$v_{p_i}(m_0^t-1)=\beta_i+v_{p_i}(t)=b\alpha_i$成立.

因而我们找到了可以使方程成立的 a、b、c，即 b 取足够大的正整数，

$a=\prod_{i=1}^{s}(p_i-1)\,p_i^{b\alpha_i-\beta_i}$，$c=\frac{m^{\prod_{i=1}^{s}(p_i-1)p_i^{b\alpha_i-\beta_i}}}{n^b}$.命题证毕.