查看: 50 | 回复: 7

[数论] $p\mid n^3-3n-1 \implies p=3\vee p\equiv\pm1\pmod 9$ [复制链接]

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

发表于 2023-10-21 00:37 1# 电梯直达

本帖最后由 业余的业余 于 2023-10-21 00:53 编辑

令 p 为 n^3-3n-1 (n 为整数) 的质因数. 求证 $p=3$ 或 $p\equiv\pm1\pmod 9$.

这题应该有些难度。还没有开始想。要求模拟这样一个例子:

定理: 令 p 为 n^3+n^2-2n-1 (n 为整数) 的质因数.则 $p=7$ 或 $p\equiv\pm1\pmod 7$
证明:有这样的 $n\in\mathbb F_p$ 满足 $n^3+n^2-2n-1=0$. 令 $\alpha\in\mathbb F_{p^2}$ 为 x^2-nx+1 的根，那么 $\alpha\ne0$ 且 $n=\alpha+\alpha^{-1}$. 我们有
$0=(\alpha+\alpha^{-1})^3+(\alpha+\alpha^{-1})^2-2(\alpha+\alpha^{-1})-1$
$\quad=\alpha^3+3\alpha+3\alpha^{-1}+\alpha^{-3}+\alpha^2+2+\alpha^{-2}-2(\alpha+\alpha^{-1})-1$
$\quad=\alpha^3+\alpha^2+\alpha+1+\alpha^{-1}+\alpha^{-2}+\alpha^{-3}$
两边同乘以 $\alpha^3(\alpha-1)$有

$$\alpha^7-1=0$$

故 α在 $\mathbb F_{p^2}$中的度（还是秩? order) $o(\alpha)$ 整除7。以下自然。

这个有趣的结论成立的关键在于对多项式 $f(x)=x^3+x^2-2x-1$, 我们有

$$f(x+x^{-1})=x^{-3}\Phi_7(x).$$

因 $\Phi_m(x)$是reciprocal, 故对任意 $m\ge2$, 存在$f(x)\in\mathbb Z[x]$ 使得

$$f(x+x^{-1})=x^{-\phi(m)/2}\Phi_m(x).$$

Cyclotomic polynomial

收藏 淘帖 1

相关帖子

- 分圆多项式基本性质
- $\mathbb Z^\times_{2n+1}$倍角的余弦之和

回复 举报

---

hbghlyj 2415 主题 5736 回帖 4万 积分 只看该作者 发消息

发表于 2023-10-21 01:09 2#

> 令 $\alpha\in\mathbb F_{p^2}$ 为 x^2-nx+1 的根

如何證明存在根

回复 举报

---

hbghlyj 2415 主题 5736 回帖 4万 积分 只看该作者 发消息

发表于 2023-10-21 01:42 3#

https://artofproblemsolving.com/community/c6h1910442p13099166
https://math.stackexchange.com/questions/3800911
https://math.stackexchange.com/questions/3989610
https://artofproblemsolving.com/ ... 20h2215443p16802675
https://artofproblemsolving.com/community/c6h2088712p15083204
https://artofproblemsolving.com/community/c6h1412003p7937406
https://artofproblemsolving.com/community/c7h2210278p16721046

评分

参与人数 1	威望 +2	理由
业余的业余	+ 2	博闻第一!

查看全部评分 收起

回复 1 举报

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

楼主 | 发表于 2023-10-21 04:31 来自手机 4#

天哪，你太厉害了。好像方向刚好相反，看来是个重要条件。

回复 举报

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

楼主 | 发表于 2023-10-21 04:32 来自手机 5#

> hbghlyj 发表于 2023-10-21 01:09
> 如何證明存在根

根的存在性有个定理。如果老兄有兴趣，回头我把证明整理上来。

回复 1 举报

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

楼主 | 发表于 2023-10-22 21:28 6#

本帖最后由 业余的业余 于 2023-10-23 01:10 编辑

用这个帖子整理下分圆多项式(cyclotomic polynomial)的知识。这个我基本是跳过了的，回头整理下，也算是给自己补漏，并希望有微益于有缘人。

基本上现在在做的事是证明Dirichlet的这么个定理（的一些特殊情形)。

> 设 a 和 m 为互质的整数，那么存在无限多的整数 k 使得 $mk+a$ 为质数。

我们用欧几里德证明有无限多质数的那么个思路或者说套路，证明这个定理的一些特例，比如 $4k\pm1$.

以$4k-1$型为例,欧式套路需要两点
1. 每个大于2（这是个摆设，多数应用下都是恒真的)的 $4k-1$ 型的整数都有一个 $4k-1$ 型的质因数；
2. 设法构造一个两两互质的无穷整数数列，让数列中的每一项都是 $4k-1$ 型的。

随着情况越来越复杂，需要不断地往工具箱里添加新的武器。比如证明形如$qk+1$(其中q为质数)的质数有无穷多个时，就引入了分圆多项式（的特殊情形)。

要往欧式套路上引，最主要的工作是构造一个两两互质的无穷数列，其中每一项都含有$qk+1$型的质因数。我们希望有一个工具来检验一个质数p，看它用质数q 取模时，是否是余 1。分圆多项式隆重登场。

> [特殊情形] q 是一个质数时，定义第q个**分圆多项式**为
> $$\Phi_q(x)=\frac{x^q-1}{x-1}=x^{q-1}+x^{q-2}+\cdots+1.$$

我们有如下命题

> 令 q 为奇素数。若对某个整数 n有质数 p 整除 $\Phi_q(n)$, 那么 $p\equiv1\pmod q$ 或 $p=q$.
>
> 形式化的表述为:
> $p,q\in\{\text{奇素数}\}\wedge\exists_{n\in\mathbb Z}(p\mid\Phi_q(n))\implies p\equiv1\pmod q\vee p=q$

证明: 因为 $\Phi_q(n)\mid n^q-1$, 我们有 $p\mid n^q-1$, 故 $o_p(n)\mid q$ 。那么$o_p(n)=1$ 和 $o_p(n)=p$ 必居其一。

若 $o_p(n)=q$，显然有 $p\equiv1\pmod q$.

若 $o_p(n)=1$，则 $n\equiv1(mod p)$ 这时

$$\Phi_q(n)\equiv1^{q-1}+\cdots+1\equiv q\pmod q.$$

这意味着 $p\mid q$, 从而 $p=q$.

证毕

> 补充说明: (定义) **整数 n 模 m 的阶**
> 当 $\gcd(n,m)=1$ 时，我们称满足 $n^d\equiv1\pmod m$ 的最小正整数 d 为 **整数 n 模 m 的阶**，记为 $o_m(n)$.

有了分圆多项式这个工具，我们就可以构造对$qk+1$型的欧式证法的无穷数列了。

为消除可能的 $p=q$ 的情形，我们令 $a_1=\Phi_q(q),a_{n+1}=\Phi_q(qa_1a_2\cdots a_n)$. 这样就构造出了两两互质，且每个元素都包含$kq+1$型质数的无穷数列，从而证明了 $qk+1$ 型素数无穷。

回复 举报

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

楼主 | 发表于 2023-10-23 01:10 7#

本帖最后由 业余的业余 于 2023-10-23 03:21 编辑

现在考虑 $qk+1$ 其中 q 不是质数。

$o_p(a)=q\implies p\equiv1\pmod q$ 继续成立。其难点在于找到多项式 $\Phi_q(x)$ 使其根模 p 的阶正好是 q, 而不是 q 的某个真约数。可以试一下，在 $\mathbb Z[x]$中找这个多项式有些棘手。办法是跳出整数甚至实数的限制，在复数域中，x^q-1 可因式分解为:

$$x^q-1=\prod_{k=1}^q(x-\zeta_q^k).$$

其中 $\zeta_q=e^{2\pi i/q}$, 是单位数(1)的第q个原始根。ζ_q^k 均匀地分布在单位圆上，这大概是分圆多项式得名的原因。这个跳出 $\mathbb Z$ 进到 $\mathbb C$的做法和后面的 跳出$\mathbb F_p[x]$进到某个$\mathbb F_{p^n}[x]$ 的处理如出一辙。两个对照着看更容易理解。

我们来看看 ζ_q^k 的阶，即满足 $\zeta_q^kd=1$ 的最小正整数，记为 $o(\zeta_q^k)$.我们有

$$\zeta_q^{kd}=1\Leftrightarrow q\mid kd\Leftrightarrow\frac{q}{\gcd(q,k)}\mid\frac{k}{\gcd(q,k)}d\Leftrightarrow\frac{q}{\gcd(q,k)}\mid d$$

故有 $o(\zeta_q^k)=q/\gcd(q,k)$. 当且仅当 $\gcd(q,k)=1$ 时，这个阶为 q. 于是有如下定义

> 第q分圆多项式
> $$\Phi_q(x)=\prod_{\substack{1\le k\le q\\ \gcd(q,k)=1}}(x-\zeta_q^k).$$

hbghlyj 探讨了分圆多项式基本性质，等我比较下看有没有什么需要补充的。

回复 举报

业余的业余 41 主题 276 回帖 2229 积分 只看该作者 发消息

楼主 | 发表于 2023-10-24 06:35 8#

> 业余的业余 发表于 2023-10-23 01:10
> 现在考虑 $qk+1$ 其中 q 不是质数。
> $\newc ...

1楼问题：
https://math.stackexchange.com/q ... which-divide-n3-3n1

这个帖子对我有一些启发。

一度以为题目错了，怎么可能 n^3-3n-1 和 n^3-3n+1 都是 $p=3$ 或 $p\equiv\pm1\pmod 9$ 呢？

用电子表格测试了一些数据发现还真这么邪门。

模拟一楼的套路，

We have some $n\in\mathbb F_p$ such that $n^3-3n-1=0$. Let $\alpha\in\mathbb F_{p^2}$ be a root of x^2-nx+1. Then $\alpha\ne0$ and $n=\alpha+\alpha^{-1}$. Now

$$\begin{aligned}0&=(\alpha+\alpha^{-1})^3-3(\alpha+\alpha^{-1})-1\\&=\alpha^3-1+\alpha^{-3} &(1)\\(1)\times\alpha^3\implies 0&=\alpha^6-\alpha^3+1 &(2)\\(2)\times\alpha^3\implies 0&=\alpha^9-\alpha^6+\alpha^3 &(3)\\(2)+(3)\implies \alpha^9&=-1 &(4)\\\implies\alpha^{18}&=1\end{aligned}$$

We have $o(\alpha)\nmid9$ and $o(\alpha)\mid18$. Let A denote the set of possible $o(\alpha)$. We have $1,3,9\notin A$ as they divide 9 which is not $o(\alpha)$. We are left with $\{2,6,18\}$. Let's examine them one by one.
i. When $o(\alpha)=2$. By $\alpha^2=2$ and $\alpha^9=-1$, we have $\alpha=-1\implies\alpha^3=-1$. Plug $\alpha^6=1$ and $\alpha^3=-1$ into (2), we get $0=3$. This has to mean the characteristic of F_p^2, p, is 3;

ii. When $o(\alpha)=6$, we have $\alpha^6=1$ and $\alpha^9=-1$, hence $\alpha^3=-1$. This is the same as the above case, so again we have $p=3$;

iii. When $(\alpha)=18$. We have $18\mid p^2-1$. In the mean time, we obviously have $2\nmid n^3-3n-1$, so p^2-1 is even. Consequently
$18\mid p^2-1\iff 9\mid p^2-1\implies\exists_{k\in\mathbb Z}(9k=p^2-1)\implies 0\equiv p^2-1\pmod 9\implies p^2\equiv1\pmod 9\implies p=\pm1\pmod 9$.

In conclusion, we have $p=3$ or $p\equiv\pm1\pmod 9$.

回复 举报