Thm1) 임의의 자연수 $n$과 정수 $x$에 대해 $\dfrac{x \cdot (x+1) \cdots (x+n-1)}{n!}$은 정수이다.

증명: $\mathbb{Z} \ni CLSUBx+n-1_{x-1} = \dfrac{(x+n-1)!}{n!x!}$ 이므로 증명된다.

Thm2) $\alpha$가 유리수가 아니고 어떤 정수계수 다항식의 근이라면,
$p(\alpha)=0$ and $p(x)=0$의 근들은 유리수가 아니고 모두 다르게 되는
정수계수 다항식 $p(x)$가 존재한다.

ex) $i \leftrightarrow x^2+1$, $\sqrt{2}+\sqrt{3} \leftrightarrow x^4-10x^2+1$

Thm3) $a, \beta$가 대수적 수이면 $\alpha+\beta$와 $\alpha\beta$도 대수적 수이다.

Thm4) (대칭다항식의 기본정리)
정수계수다항식 $f(x_1, \ldots, x_n)$이 대칭다항식이면 어떤 정수계수 다항식 $p(x_1, \ldots, x_n)$이
존재하여 $f(x_1, \ldots, x_n) = p(e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n))$을 만족한다.
이때 $\deg f \geq \deg p$ 이다.

ex) $x^2+y^2+z^2 = (x+y+z)^2 - 2(xy+yz+zx)$, $x^2y+xy^2 = (x+y)xy$.

Thm5) 소수의 개수는 무한하다.

Step 1.

$e^{z_1}+1=0$을 만족하는 $z_1$이 대수적 수라고 가정하자. 그러면 $z_1$을 근으로 가지는 정수계수 기약다항식 $p(x)$가 존재한다. $p(x)=0$의 모든 근을 $z_1,...,z_n$이라고 하자. 그러면

$(e^{z_1}+1)(e^{z_2}+1)\cdots(e^{z_n}+1)=0$ 이 성립한다.

$X=\{a_1z_1+\cdots+a_nz_n : a_i=0 \text{ or } 1\,,\, i=1,...,n\}$로 정의하자.

이때 가능한 $X$의 원소는 $2^n$개이고, 그들이 서로 다를 필요는 없다.

그러면 위 등식으로부터 $\sum_{w\in X} e^w=0 \ \cdots$ (ㄱ)을 얻는다.

차수가 $m$인 다항식을 $f(z)$라 하자.

그리고 $F(z)=f(z)+f'(z)+\cdots+f^{(m)}(z)$로 정의하자.

그러면 $\frac{d}{dz}\left(e^{-z}F(z)\right)=-e^{-z}f(z)$가 성립한다.

따라서 임의의 $w\in\mathbb{C}$에 대해 $e^{-w}F(w)-F(0)=-\int_0^w e^{-z}f(z)dz$

$$\Leftrightarrow\ F(w)-e^wF(0)=-\int_0^w e^{w-z}f(z)dz$$ 를 얻는다.

이때 저 등식 양 변에 $\sum_{w\in X}$를 취하면

(ㄱ)에 의해 $\sum_{w\in X}F(w)=-\sum_{w\in X}\int_0^w e^{w-z}f(z)dz \ \cdots$ (ㄴ)를 얻는다.

앞으로 우리는 $f(z)$에 적절한 정수계수 다항식을 대입하여 (ㄴ)의 좌변은 음이 아닌 정수이지만 우변은 0에 충분히 가까운 상황을 만듦으로써 모순을 이끌어 낼 것이다.

Step 2.

위에서 $p(x)$의 최고차항의 계수를 $a$라 하고,

소수 $p$에 대해 $g(t)=t^{p-1-pq}a^{pd+\beta}\prod_{\zeta\in X}(t-\zeta)^p$로 정의하자.

이때 $q$는 $X$의 원소 중 0이 아닌 것의 개수이고 $d=2^n$이다.
그러면 기본대칭함수 $e_1,...,e_d$에 대해,

$$g(t)=t^{p-1-pq}a^{pd+\beta}(t^d-e_1(\zeta_1,...,\zeta_d)t^{d-1}+\cdots+(-1)^d e_d(\zeta_1,...,\zeta_d))^p$$
$$=t^{p-1-pq}(a^\beta(at)^d-a^\beta a e_1(\zeta_1,...,\zeta_d)(at)^{d-1}+\cdots+a^\beta(-a)^d e_d(\zeta_1,...,\zeta_d))^p$$

가 성립함에 주목하자.
그런데 이때 각 $i=1,...,d$에 대해 $a^{i+\beta}e_i(\zeta_1,...,\zeta_d)$는 정수이다.
왜냐하면 $e_i(\zeta_1,...,\zeta_d)$는 $(z_1,...,z_n)$에 대한 대칭 다항식이기 때문에
$e_i(\zeta_1,...,\zeta_d)=T_i(e_1(z_1,...,z_n),...,e_n(z_1,...,z_n))$을 만족하는 정수계수다항식 $T_i$가 존재하고
$p(x)$의 각 계수들이 $\pm a e_i(z_1,...,z_n)$이므로 이들은 정수인데
$\beta$가 충분히 크므로 $a^{i+\beta}T(e_1(z_1,...,z_n),...,e_n(z_1,...,z_n))$은 역시 정수이다.
즉, $g(t)$는 정수계수 다항식이다.

Step 3.

위에서 $X$의 원소들 중 0인 것의 개수가 $q$라는 것에 주목하여 $g$를 아래와 같이 표현하자.
$g(t)=r_m(at)^m+r_{m-1}(at)^{m-1}+\cdots+r_p(at)^p+r_{p-1}(at)^{p-1}$.

이때 $m=p(d-q+1)-1$이고 각 $i$에 대해 $r_i$는 정수이다. 특히, $r_{p-1}=a^{\beta}\prod_{0\neq\zeta\in X}\zeta^p$.

$1\le i\le p-2$일 때 $g^{(j)}(0)=0$,

$i=p-1$일 때 $g^{(i)}(0)=a^p(p-1)!r_{p-1}=(p-1)!a^{\beta}\prod_{0\neq\zeta\in X}(a\zeta)^p$이다.

또한, $0\neq\zeta\in X$에 대해 $g$는 $(t-\zeta)^p$를 인수로 가지므로
$1\le i\le p-1$이면 $g^{(i)}(\zeta)=0$이다.

한편 $p\le i$인 경우는 $g^{(i)}(t)=\sum_{s=0}^{m-i}\frac{(m-s)!}{(m-i-s)!}r_{m-s}(at)^{m-i-s}a^{\beta}$이 되므로

$\sum_{0\neq\zeta\in X}g^{(i)}(\zeta)=\sum_{s=0}^{m-i}\frac{(m-s)!}{(m-i-s)!}r_{m-s}\left(a^{m-i-s}\sum_{0\neq\zeta\in X}\zeta^{m-i-s}\right)$가 성립한다.

이때 $\sum_{0\neq\zeta}\zeta^{m-i-s}$는 $0\neq\zeta$인 $\zeta$들에 대한 대칭다항식이므로 Step 2의 중간과정과 비슷한

방법으로 $a^{\beta}a^{m-i-s}\sum_{0\neq\zeta}\zeta^{m-i-s}$가 정수임을 얻는다. $r_{m-s}$와 $\frac{(m-s)!}{(m-i-s)!}$역시 명백하게

정수이므로 $p\le i$일 때 $\sum_{0\neq\zeta\in X}g^{(i)}(\zeta)$는 정수이다. 그리고 소수 $p$를 약수로 가진다.

따라서 위 Step 1에서 (ㄴ)의 좌변은 $\sum_{i\ge p}\sum_{0\neq\zeta\in X}g^{(i)}(\zeta)+a^{\beta+p}(p-1)!\left(\prod_{0\neq\zeta\in X}\zeta\right)^p$ 이다.

그런데 소수 $p$를 충분히 크게 택하면 $a$, $\prod_{0\neq\zeta\in X}\zeta$와 모두 서로소이게 할 수 있으므로
$p$가 충분히 크면 (ㄴ)의 좌변은 $p$를 나누지 않는 정수가 된다. 즉, 0이 아닌 정수이다.

그리고 위 증명을 잘 살펴보면 $\sum_{0\neq\zeta\in X}g^{(i)}(\zeta)$도 $(p-1)!$을 인수로 가지므로 $(i\ge p)$
결과적으로 (ㄴ)의 좌변은 $(p-1)!$을 소인수로 가진다.

따라서 우리는 최종적으로 (ㄴ)에 $g$대신 $f(t)=\frac{g(t)}{(p-1)!}$를 대입한다.

Step 4.

위에서 (ㄴ)에 $g$대신 $f$를 대입하면 $I_m(z) = \frac{1}{(p-1)!}\int_0^z e^{z-t}g(t)dt$이 된다.

임의의 $0 \neq \zeta \in X$에 대해 $I_m(\zeta) = \frac{1}{(p-1)!}\int_0^\zeta e^{\zeta-t}g(z)dz$를 생각하자.

이때 $\zeta$를 포함하는 반지름이 $r_\zeta$인 적당한 disk $D_\zeta$를 생각하면

$\left|\int_0^\zeta e^{\zeta-t}g(z)dz\right| \leq |\zeta|e^{2r}M$ $(M = \max\{|g(z)| : z \in D_\zeta\}$ 이다.

이때 $g(t) = t^{p-1-pq}a^{pd+\beta}\prod_{\zeta\in X}(t-\zeta)^p$ 임을 상기하면, $M \leq (2r)^{p-1-pq}|a|^{pd+\beta}2^d r^p$ 이다.

그런데 임의의 양수 $x$에 대해 $\lim_{n\to\infty}\frac{x^n}{n!} = 0$이므로 소수 $p$가 충분히 크면

$\frac{M}{(p-1)!}$이 충분히 0에 가까워진다. 따라서 $\frac{I_m(\zeta)}{(p-1)!}$도 0에 충분히 가까워진다.

이는 임의로 $X$에서 뽑은 $\zeta$에 대해 성립하고 $X$가 유한하므로,

결국 소수 $p$가 충분히 크면 (ㄴ)의 좌변이 0에 가까워지게 되어 증명이 끝난다.