数论　　牛力明　30212330ΨΨ

2.1 在 $[2, n]$ 中考虑与 ~~其中所有素数~~ $p_1, \cdots, p_k$ 不相关的数.

~~运用容斥原理可知~~: 注意到, 素数 $p \mid n! \iff p = p_i, 1 \le i \le k$.

以及 $V_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] \le \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{\frac{n}{p}}{1-\frac{1}{p}} = \frac{n}{p-1}$

从而 $n! = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \le p_1^{\frac{n}{p_1-1}} \cdots p_k^{\frac{n}{p_k-1}}$

$\Rightarrow \ln n! \le \sum_{i=1}^{k} \frac{n}{p_i-1} \ln p_i = n \sum_{i=1}^{k} \frac{\ln p_i}{p_i-1}$

$\Rightarrow \frac{\ln n!}{n} \le \sum_{i=1}^{k} \frac{\ln p_i}{p_i-1} \le k \ln 2$

没想好… 由素数定理 $\pi(x) \sim \frac{x}{\ln x}$ 可知在 $[2, x]$ 中素数占比约为 $\frac{1}{\ln x}$, 在 x 充分大时趋于 0.

2.2 取 $n > k$, 则 $n!+2, n!+3, \cdots, n!+(k+1)$ 即可.

2.3 $(a_1, \cdots, a_n) = x_1a_1 + x_2a_2 + \cdots + x_na_n$, 其中 $x_i \in \mathbb{Z}$.

归纳. $n=2$ 已证. 设 $n-1$ 时成立, n 时:

$(a_1, \cdots, a_n) = ((a_1, \cdots, a_{n-1}), a_n)$

$= y_1(a_1, \cdots, a_{n-1}) + y_2a_n$

$= y_1(x_1a_1 + \cdots + x_{n-1}a_{n-1}) + y_2a_n$

$= y_1x_1a_1 + \cdots + y_1x_{n-1}a_{n-1} + y_2a_n$. 即证.

2.4. $\forall n \in \mathbb{Z}$, 若不存在素数 $p < n$, 使 $p \mid n \Rightarrow n$ 素, 已分解.

否则 $p \mid n$, $\Rightarrow n = pq$. 依此进行下去即可.

可得到 n 的一个素因数分解.

唯一性: 设 $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} = q_1^{\beta_1} \cdots q_s^{\beta_s}$.

由 $p_1 \mid q_1^{\beta_1} \cdots q_s^{\beta_s}$, 可知 $\exists q_i^{\beta_i}$ 使 $p_1 \mid q_i^{\beta_i} \Rightarrow p_1 \mid q_i$, 即 $p_1 = q_i$ (反复用 2.6)

采用归纳法, $n=1,2,3,4,5$ 易于验证. 设小于 n 时成立, n 时,

由 $\frac{n}{p_1} = p_1^{\alpha_1-1} \cdots p_t^{\alpha_t} = \frac{n}{q_i} = q_1^{\beta_1} \cdots q_i^{\beta_i-1} \cdots q_s^{\beta_s}$

$\Rightarrow p_1^{\alpha_1-1} \cdots p_t^{\alpha_t}$ 与 $q_1^{\beta_1} \cdots q_i^{\beta_i-1} \cdots q_s^{\beta_s}$ 同一分解.

$\Rightarrow n$ 也只有唯一分解.

2.5 反例: $3 \times 2 \equiv 6 \times 2 \pmod 6$, $2 \equiv 2 \pmod 6$, $(2,6) = 2$.

$\Rightarrow$ 但 $3 \not\equiv 6 \pmod 6$.

证明: 由 $(c, m) = 1 \Rightarrow \exists u, v \in \mathbb{Z}, uc + vm = 1 \Rightarrow uc \equiv 1 \pmod m$

而 $ac \equiv bd \pmod m \Rightarrow acu \equiv bdu \pmod m$

$\Rightarrow a \equiv b \pmod m$.

2.6 归纳. $n = 0,1,2,3,4$ 可验证. 设 n 时成立, $n+1$ 时.

$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1$

$= (n^5 - n) + 5n^4 + 10n^3 + 10n^2 + 5n$

$\equiv n^5 - n \pmod 5$. 即证.

2.7 只用对素数幂次证明, 即 $\varphi(p^\alpha q^\beta) = \varphi(p^\alpha)\varphi(q^\beta)$.

而在 $0, 1, \cdots, p^\alpha q^\beta - 1$ 中, 与 $p^\alpha q^\beta$ 互素的即不被 p, q 整除的

被 p 整除: $p^{\alpha-1}q^\beta$ 个. 被 q 整除 $p^\alpha q^{\beta-1}$ 个. 被 pq 整除: $p^{\alpha-1}q^{\beta-1}$ 个.

$\Rightarrow \varphi(p^\alpha q^\beta) = p^\alpha q^\beta - p^{\alpha-1}q^\beta - p^\alpha q^{\beta-1} + p^{\alpha-1}q^{\beta-1}$

$= p^\alpha q^\beta (1-\frac{1}{p})(1-\frac{1}{q})$

$= \varphi(p^\alpha)\varphi(q^\beta)$

设 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

有 $\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1}(1-\frac{1}{p_1}) \cdots p_k^{\alpha_k}(1-\frac{1}{p_k}) = m(1-\frac{1}{p_1}) \cdots (1-\frac{1}{p_k})$.

2.8 $\sum_{d \mid m} \varphi(d) = \sum_{\substack{0 \le i_1 \le \alpha_1 \\ \vdots \\ 0 \le i_k \le \alpha_k}} \varphi(p_1^{i_1} \cdots p_k^{i_k}) = \sum_{0 \le i_1 \le \alpha_1} \cdots \sum_{0 \le i_k \le \alpha_k} (\varphi(p_1^{i_1}) \cdots \varphi(p_k^{i_k}))$

$= \prod_{j=1}^{k} \left(\sum_{0 \le i_j \le \alpha_j} \varphi(p_j^{i_j})\right) = \prod_{j=1}^{k} p_j^{\alpha_j} = m$.

2.9 定理证明: $M = \{0, 1, \cdots, m-1\}$. $\forall x \in M$. 考虑 $x \equiv x_i \pmod{m_i}$

并将 x 对应到 $(x_1, \cdots, x_n) \in M'$

能注意到, 若 $x \longrightarrow (x_1, \cdots, x_n)$, $y \longrightarrow (y_1, \cdots, y_n)$

且 $(x_1, \cdots, x_n) = (y_1, \cdots, y_n)$, 则 $x \equiv y \pmod{m_i}$.

$\Rightarrow m \mid x-y$. $\Rightarrow x-y=0$. $\Rightarrow x=y$. 从而单. 又 $|M| = |M'| \Rightarrow$ 双射.

从而 $\forall (a_1, \cdots, a_n) \in M'$, 存在唯一 $x \in M$ 与之对应.

求解过程: 令 $d_i = \frac{m}{m_i}$, 由 $(d_i, m_i) = 1$, $\Rightarrow \exists d_i^{-1} \in \mathbb{Z}$, $d_id_i^{-1} \equiv 1 \pmod{m_i}$.

令 $x = \sum_{i=1}^{n} d_id_i^{-1}a_i$, 则由 $i \ne j$ 时, $d_i \equiv 0 \pmod{m_j}$

$\Rightarrow x \equiv d_id_i^{-1}a_i \equiv a_i \pmod{m_i}$. 故 x 为该方程组根.

2.10 构造对应关系 $a \longrightarrow (a_0, a_1, \cdots)$ $0 \le a_i < b-1$.

$a \equiv a_0 \pmod b$.

$\frac{a-a_0}{b} \equiv a_1 \pmod b$

$\vdots$

可得到一个映射.

若 $x \to (x_0, x_1, \cdots)$, $y \longrightarrow (y_0, y_1, \cdots)$

$(x_0, \cdots) = (y_0, \cdots)$, 展开可知 $x = y$. $\Rightarrow$ 单射.

关于满射: $\forall (x_0, x_1, \cdots)$. 可令 $x = x_0 + x_1b + \cdots$

则 x 即对应到此.

从而是双射 $\Rightarrow$ 唯一对应.

(事实上由于 b 进制唯一立得).

数论　　牛少明　　3021233044.

2.11 ① $x^2\equiv 7 \pmod{227}$

$\left(\frac{7}{227}\right)\left(\frac{227}{7}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{227-1}{2}}=1$

$\left(\frac{227}{7}\right)=\left(\frac{3}{7}\right)=-1 \Rightarrow$ 无解.

2. $(11x)^2\equiv -66 \pmod{91}$.
$\equiv 25$　　有解.

2.12. $\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=\sum_{x=1}^{p}\left(\frac{x}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)+\left(\frac{p}{p}\right)=0+1=1$.（二次剩余与非二次剩余都有 $\frac{p-1}{2}$ 个）.

2.13 事实上，1,4,p 都是二次剩余...

~~反设不行，则二次剩余 {1,3,5,...}~~
~~非二次剩余 {2,4,6,...}.~~
~~矛盾，因为4是二次剩余.~~

反证法 $\Rightarrow$ 2,5,10 不是二次剩余

$\left(\frac{10}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$

$\Rightarrow -1=(-1)\cdot(-1)$，矛盾.

2.14 反设不行，则有由 1,4 是二次剩余

$\Rightarrow$ 2不是，3不是，6不是

~~在1~p-1中，二次剩余只能相邻两个一起出现~~ ~~(因为二次剩余与非二次剩余一样多)~~.

~~除此之外两个二次剩余之间至少有2个非二次剩余.~~

~~{1,3} {2,4}~~ ~~设有x个二次剩余对，y个单个二次剩余~~

~~$\Rightarrow 2x+y=\frac{p-1}{2}$.~~

$\Rightarrow \left(\frac{2}{p}\right)=-1,\ \left(\frac{3}{p}\right)=-1 \Rightarrow \left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1$，矛盾.

作业 3.3　　牛少明　3021233044

若 $1\in T$ 且 $d(T)=\lim\limits_{n\to\infty}\frac{f(n)}{n}>0$. 那么T有正密率.

证明：由 $\lim\limits_{n\to\infty}\frac{f(n)}{n}$ 存在. 设 $\lim\limits_{n\to\infty}\frac{f(n)}{n}=\alpha$.

取 $\varepsilon=\frac{\alpha}{2}$, 则 $\exists N$, $n>N$ 时, $\left|\frac{f(n)}{n}-\alpha\right|<\frac{\alpha}{2}$. $\Rightarrow \frac{f(n)}{n}>\frac{\alpha}{2}$.

又 $f(n)\geqslant 1$.

$\Rightarrow$ 取 $\beta=\min\{\frac{\alpha}{2},\frac{1}{N}\}$.

即有 $f(n)\geqslant\beta n$.

($n\leqslant N$ 时, 有 $\frac{f(n)}{n}\geqslant\frac{1}{N}\geqslant\beta$,

$n>N$ 时, $\frac{f(n)}{n}>\frac{\alpha}{2}\geqslant\beta$).

作业 4.1　证: $1+\frac{1}{2}+\cdots+\frac{1}{n}\notin\mathbb{Z}$.

证: 即 $\frac{n!+\frac{n!}{2}+\cdots+\frac{n!}{n}}{n!}\notin\mathbb{Z}$. 反设是整数.

考虑 $p^r\leq n<p^{r+1}$.

则 $V_p(\frac{n!}{p^r})<V_p(\frac{n!}{k})$, $\forall\ k\neq p^r, 1\leq k\leq n$.

($\Leftrightarrow V_p(k)<V_p(p^r)=r$, 成立).

从而有: $n!+\frac{n!}{2}+\cdots+\frac{n!}{n}=V_p(\frac{n!}{p^r})\left(p\cdot M+\underbrace{\frac{n!}{p^r q}\cdot\frac{1}{p^{V_p(\frac{n!}{p^r})}}}_{\text{不被}p\text{整除}}\right)$.

$\Rightarrow V_p(n!+\cdots+\frac{n!}{n})=V_p(\frac{n!}{p^r})<V_p(n!)$.

矛盾. (取 $p=2$ 即可).

作业4.2　$\lim\limits_{n\to\infty}\frac{p_n}{n\ln n}=1$

证明: 由 $\pi(p_n)=n$. 知 $\cancel{\lim\limits_{n\to\infty}}$ $\pi(p_n)\sim\frac{p_n}{\ln p_n}$, 即 $\lim\limits_{n\to\infty}\frac{n\ln p_n}{p_n}=1$.

$\Rightarrow$ 只用证: $\lim\limits_{n\to\infty}\frac{\ln p_n}{\ln n}=1$.

可证更强的 $\lim\limits_{n\to\infty}\frac{\ln n}{\ln\pi(n)}=1$. ($p_n$是$n$子列).

由 $\cancel{\lim\limits_{n\to\infty}}$ $\cancel{\ln\pi(n)}$ $0\leq 1-\frac{\ln\pi(n)}{\ln n}=\frac{\ln\frac{n}{\pi(n)}}{\ln n}$

$\frac{n}{\pi(n)\ln n}\to 1\Rightarrow\exists N, n>N, \frac{n}{\pi(n)\ln n}<1+\varepsilon\Rightarrow\frac{n}{\pi(n)}<(1+\varepsilon)\ln n$.

$\Rightarrow \ln\frac{n}{\pi(n)}<\ln[(1+\varepsilon)\ln n]\Rightarrow 0\leq\frac{\ln\frac{n}{\pi(n)}}{\ln n}\leq\frac{\ln[(1+\varepsilon)\ln n]}{\ln n}\to 0$

从而 $\lim\limits_{n\to\infty}\frac{\ln\pi(n)}{\ln n}=1$. $\Rightarrow\lim\limits_{n\to\infty}\frac{\ln n}{\ln\pi(n)}=1$. 从而得证!