Homework 6

李昊宸

2018.12.24

1.

证明：记 $A=\{1,2，\ldots,p-1\}$

充分性：

若 p 不是素数，那么 A 中有 p 的因子，于是有 $\gcd((p-1)!,p)=a\neq 1$

记 $p=ac,(p-1)!=ad$，于是 $(p-1)!\equiv a[d-kc](\mathrm{mod}\ p=ac)\equiv b(\mathrm{mod}\ p)$，其中 k 满足

d-kc>0， d-(k+1)c<0

所以 a|b

因 $a\neq 1,$所以$a\nmid -1,$故$b\nmid -1$

必要性：

A 中元素在模 p 的意义下构成乘法群，每一个元素 a 都存在逆元 a^{-1}，满足 $aa^{-1}=1$（mod p）

由于两个互为逆的元素相乘等于 1，下面我们寻找逆等于自身的元素

$a^2\equiv 1(\mathrm{mod}\ p)\Leftrightarrow(a+1)(a-1)\equiv 0(\mathrm{mod}\ p),$得$a_1=1,a_2=p-1$

于是 $(p-1)!\equiv 1\times(p-1)\equiv -1(\mathrm{mod}\ p)$

2．

p>2 时，欧拉判别法：

$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}(\mathrm{mod}\ p),\left(\frac{b}{p}\right)=b^{\frac{p-1}{2}}(\mathrm{mod}\ p),\left(\frac{ab}{p}\right)=(ab)^{\frac{p-1}{2}}(\mathrm{mod}\ p),$

因 $\left|\left(\frac{ab}{p}\right)-\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right|\leq 2,p>2$，于是 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

P=2 时只有两种情况：$\left(\frac{1}{2}\right)=1,\left(\frac{-1}{2}\right)=-1$,此时也满足等式。

综上，等式得证

3.

证明：

假设命题错误，即不存在这样的两个球，使每个都满足新盒子中的球的个数比旧盒子中的更少

考虑 m=n+1 的场合

由抽屉原理，必有两个球放在同一个盒子内，于是这两个球在原盒子中的个数大于等于 2

放入新盒子中，每个盒子内都只有一个球，于是这两个球满足命题的内容，这与假设不存在

矛盾！于是在 m=n+1 时结论成立
假设 m=k 时命题正确，m=k+1 时，相当于向 k 的情况中加入一个球，加入这个球后，至少有两个球在原盒子中的个数增加 1，放入新盒子中，若这两个球仍在同一个盒子，那么可将这两个球看作同一个球，采用 m=k 时的命题可得；若这两个球不在同一个盒子，那么可将这个新球与原来不与它在同一个盒子里的球现在在同一个盒子里的球组队，使用 m=k 时的命题依然可得。

4.

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}3^{\frac{p-1}{2}} \bmod p$$

P 为 6k-1 型时，由上周作业知，$\left(\frac{-3}{p}\right)=-1$

P 为 6k+1 时，
$$(\frac{3}{p})=(-1)^{\frac{2}{2}\frac{p-1}{2}}(\frac{p}{3})=(-1)^{3k}(\frac{1}{3})$$
$$=(-1)^{3k}=\begin{cases}1，\text{k为偶数}\\-1，\text{k为奇数}\end{cases}$$

所以$\left(\frac{-3}{p}\right)=1$

综上，$\left(\frac{-3}{p}\right)=\begin{cases}1, p=6k+1\\-1, p=6k-1\end{cases}$

5.
证明 8k+5 型无穷:
假设 8k+5 型素数有穷，为 p1,…，pn

令 $N=4\prod_{i=1}^{n}p_i^{\,2}+1,$设q$|N$ 。N 为 8k+5 型素数

有$\left(\frac{-1}{q}\right)=\left(\frac{N-1}{q}\right)=1$，而$\left(\frac{-1}{q}\right)=1$仅对 4k+1 型素数成立，故 q 为 8k+1 或 8k+5 型素数

设 N 的素因子只有 8k+1 型，那么 $N\equiv 1\bmod 8$，而由 N 的定义式，$N\equiv 5\bmod 8$ 矛盾!
所以 N 有 8k+5 型因子，这与假设矛盾，故 8k+5 型素数无穷。
证明 8k+1 型素数无穷:
假设 8k+1 型素数有穷，为 p1,…，pn

令 $N=16\prod_{i=1}^{n}p_i^{\,4}+1,$设q$|N$ 。N 为 8k+1 型素数

类似对 8k+5 的证明，q 只能为 8k+1 型或 8k+5 型。记 $x=2\prod_{i=1}^{n}p_i$ ，有 $x^4=-1(\bmod p)$

定理：对于 $x^n = a(\mathrm{mod}\ p)$，则 $a^{\frac{p-1}{\gcd(n,p-1)}} = 1(\mathrm{mod}\ p)$

若 q 为 8k+5 型，则 $a^{2k+1} = 1(\mathrm{mod}\, 8k+5)$，即 $(-1) = 1(\mathrm{mod}\ p)$，矛盾!

所以 8k+5 不是素因子，故素因子只有 8k+1，这又与假设矛盾！故 8k+1 型素数无穷。

6.

假设 12k+7 型素数有穷，为 p1,…，pn

令 $N = 4\prod_{i=1}^{n} p_i^{\,2} + 3$, 设$\mathrm{q} \mid N$。N 为 12k+7 型素数

有 $\left(\frac{-3}{q}\right) = \left(\frac{N-3}{q}\right) = 1$，而 $\left(\frac{-3}{q}\right) = \left(\frac{-1}{a}\right)\left(\frac{3}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{3}\right)(-1)^{\frac{q-1}{2}} = \left(\frac{q}{3}\right)$仅对 12k+1 或 12k+7 型素数成立，故 q 为 12k+1 或 12k+7 型素数

设 N 的素因子只有 12k+1 型，那么 $N \equiv 1 \bmod 12$，而由 N 的定义式，$N \equiv 7 \bmod 12$ 矛盾!

所以 N 有 12k+7 型因子，这与假设矛盾，故 12k+7 型素数无穷。

7.

$T_m = \prod_{p \le m, p \in P} p$，P 为所有小于 m 的素数的集合

则 $T_m = (\prod_{\frac{m}{2} < p \le m, p \in P} p)(\prod_{p \le \frac{m}{2}, p \in P} p)$

因为 $\prod_{p \le m, p \in P} p^{f_p(m) - 2f_p(\frac{m}{2})} = \frac{m!}{(\frac{m}{2})!(\frac{m}{2})!} = \binom{m}{\frac{m}{2}}$，故

$T_m = (\prod_{\frac{m}{2} < p \le m, p \in P} p)(\prod_{p \le \frac{m}{2}, p \in P} p) < \binom{m}{\frac{m}{2}} T_{\frac{m}{2}} \le T_{\frac{m}{2}} 2^m \le T_{\frac{m}{4}} 2^{\frac{m}{2}} 2^m \le \ldots \le 2^{2m} = 4^m$

8.

$|A+B| \ge |A| + |B| - 1$

对 B 做归纳:

当 B 为空集时，$|A| \ge |A| - 1$

当 B 为单元集时，$|A+B| = |A| \ge |A| + 1 - 1$

设 B 等于 n 元集时成立

现向 B 中加入第 n+1 个元素 b_{n+1} 构成 B'

通过调整不妨设 b_{n+1} 是 B'中最大的元素

那么 $a_{max}+b_{n+1}$ 是{A+B}中的新元素，$a_{\max} = \max\{a_i, a_i \in A\}$

于是$|A+B'|\geq|A+B|+1\geq|A|+n-1+1=A+n=|A|+|B'|-1$

原式得证