代数学基础, 2025 秋, USTC

第二周作业答案

Due: 线下提交：9.25 下课前；线上提交：9.28 24:00 前.

无论线上线下提交，均需按要求在课程主页进行操作.

姓名: ____________　　学号: ____________

Assignment 1

若 $n \in \mathbb{N}^*$，证明 $\gcd(n!+1,(n+1)!+1)=1$.

证明. 注意到 $\gcd(n!+1,(n+1)!+1) = \gcd(n!+1,(n+1)!+1-(n+1)(n!+1)) = \gcd(n!+1,-n) = \gcd(n!+1,n) = 1$. □

Assignment 2

用 Euclid 算法求 963 和 657 的最大公约数，并求方程

$$963x + 657y = \gcd(963, 657)$$

的一组特解和所有整数解.

证明. 由 Euclid 算法可得到 $\gcd(963,657)=9$，以及 $963\times 58 - 657\times 85 = 9$，所以 $(x_0,y_0)=(58,-85)$ 是方程 $963x+657y=9$ 的一组特解. 所有解 (x,y) 满足 $963(x-x_0)+657(y-y_0)=0$，即 $963(x-58)=657(85+y)$，所以 $(x,y)=(58+73t,-85-107t)$，其中 $t\in\mathbb{Z}$. □

Assignment 3

设 $a,b\in\mathbb{N}^*$，且 $\gcd(a,b)=1$. 证明当 $n>ab-a-b$ 时，方程

$$ax+by=n$$

存在非负整数解. 但当 $n=ab-a-b$ 时，方程无非负整数解.

证明. 先证存在性. 由 $\gcd(a,b)=1$, 扩展欧几里得算法给出整数解 (x_0,y_0) 使 $ax_0+by_0=1$. 乘以 n 得到 $a(nx_0)+b(ny_0)=n$. 所有整数解为

$$x = nx_0 + bt, \qquad y = ny_0 - at \qquad (t\in\mathbb{Z}).$$

我们希望选 t 使 $x, y \geq 0$. 取

$$t_0 := \min\{t \in \mathbb{Z}: \ nx_0 + bt \geq 0\},$$

则 $0 \leq nx_0 + bt_0 < b$. 令 $x = nx_0 + bt_0$，$y = ny_0 - at_0$，则

$$y = \frac{n - ax}{b}.$$

因为 $0 \leq x < b$，若 $n > ab - a - b = (a-1)(b-1) - 1$，则

$$n - ax \geq n - a(b-1) > ab - a - b - a(b-1) = -1,$$

故 $n - ax > -1$，于是 $y \geq 0$. 因此当 $n > ab - a - b$ 时存在非负整数解.

再证临界点处无解. 若存在非负整数解 $ax + by = ab - a - b$，则移项得

$$a\big((b-1) - x\big) = b(y+1).$$

由 $\gcd(a, b) = 1$ 知 a 必整除 $y+1$，设 $y + 1 = ak$（$k \in \mathbb{N}$），则

$$(b-1) - x = bk \quad \Rightarrow \quad x = (b-1) - bk = -1 - (k-1)b < 0,$$

与 $x \geq 0$ 矛盾. 故 $n = ab - a - b$ 时无非负整数解. □

Assignment 4

如果整数 $n > 2$，证明 n 到 $n!$ 之间至少有一个素数. 由此证明素数有无穷多.

证明. 令 $N = n! - 1$，取 N 的最小素因子 p. 若 $p \leq n$，则 $p \mid n!$，而 $p \mid n! - 1$ 亦必须成立，这不可能（同一素数不可能同时整除相差 1 的两数）. 故 $p > n$. 又有 $p \mid N < n!$，于是

$$n < p < n!.$$

从而在区间 $(n, n!)$ 内至少存在一个素数 p.

由此可见素数无穷多：任取 $n > 2$，总能在 $(n, n!)$ 中找到素数 $> n$，不可能存在最大的素数. □

Assignment 5: 选做 (optional)

1. 设 m 为正整数，证明：如果 $2^m + 1$ 为素数，则 m 为 2 的方幂.

2. 对 $n \geq 0$，记 $F_n = 2^{2^n} + 1$，这称为 **费马数**. 证明：如果 $m > n$，则

$$F_n \mid (F_m - 2).$$

3. 证明：如果 $m \neq n$，则 $(F_m, F_n) = 1$. 由此证明素数有无穷多个.

注记. 费马数中的素数称为 **费马素数**. 例如

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

都是素数. 费马曾经猜测所有的费马数 F_n 都是素数，但是欧拉在 1732 年证明了

$$F_5 = 641 \cdot 6700417$$

不是素数. 目前人们不知道除去前 5 个费马数外，是否还存在其他的费马素数.

证明. (1) 若 m 含有奇素因子 r，写 $m = rs$（r 为奇数，$s \geq 1$）. 利用恒等式

$$X^r + 1 = (X+1)\big(X^{r-1} - X^{r-2} + \cdots - X + 1\big) \quad (r \text{ 为奇})$$

令 $X = 2^s$，得

$$2^m + 1 = (2^s)^r + 1$$

可分解为两个大于 1 的因子，从而不是素数，矛盾. 故 m 只能是 2 的方幂.

(2) 由恒等式

$$2^{2^k} - 1 = (2^{2^{k-1}} - 1)(2^{2^{k-1}} + 1) = (F_{k-1} - 2)F_{k-1}$$

递推可得

$$F_m - 2 = (F_{m-1} - 2)F_{m-1} = \cdots = (F_0 - 2)\, F_0 F_1 \cdots F_{m-1} = -1 \cdot \prod_{j=0}^{m-1} F_j.$$

于是当 $m > n$ 时，F_n 显然整除 $F_m - 2$.

(3) 设 d 同时整除 F_m 与 F_n（$m \neq n$）. 不妨设 $m > n$. 由 (2) 知 $F_m - 2$ 被 F_n 整除，故 d 也整除 $F_m - (F_m - 2) = 2$. 但每个 F_k 都是奇数（因为 2^{2^k} 为偶数，$2^{2^k} + 1$ 为奇数），故 d 不可能为 2，只好 $d = 1$. 于是 $(F_m, F_n) = 1$.

再由 (2)(3)：$F_m - 2$ 被 $F_0, \ldots, F_{m-1}$ 的乘积整除，且这些 F_j 两两互素，因此每一个 F_m 至少引入一个新的素因子，与之前出现过的素因子不同. 故素数只能无限多. $\square$

Assignment 6: 选做 (optional)

1. 设 m, n 都是大于 1 的整数，证明：如果 m^n-1 是素数，则 $m=2$ 并且 n 是素数.

2. 设 p 是素数，记 $M_p=2^p-1$，这称为 **梅森数**. 证明：如果 p, q 是不同的素数，则
$$(M_p, M_q)=1.$$

注记. 1644 年，法国数学家梅森（Mersenne）研究过形如 $M_p=2^p-1$ 的素数，后来人们将这样的素数称为 **梅森素数**. 是否存在无穷多个梅森素数是一个悬而未决的问题. **梅森素数互联网大搜索计划**（Great Internet Mersenne Prime Search，简称 GIMPS，网址：http://www.mersenne.org/default.php）是互联网上志愿者通过使用闲置计算机 CPU 寻找梅森素数的一个合作计划. 通过此计划，人们在 2016 年 1 月 7 日找到了迄今为止最大的素数
$$M_{74207281},$$
也是已知的第 49 个梅森素数.

助教注. 课本上对 Mersenne 数的最新研究成果尚未更新. 值得指出的是，在 2024 年 10 月 21 日，GIMPS 发现了第 52 个已知的梅森素数 $2^{136279841}-1$，也是迄今为止最大的素数.

证明. (1) 因式分解
$$m^n-1=(m-1)\big(m^{n-1}+m^{n-2}+\cdots+1\big).$$
若 $m\geq 3$，则 $m-1\geq 2$ 且括号内的和 >1，从而为合数，矛盾；故 $m=2$. 再若 n 合成，设 $n=rs$（$r, s>1$），则
$$2^n-1=(2^r)^s-1=(2^r-1)\big((2^r)^{s-1}+\cdots+1\big)$$
仍为合数，矛盾. 于是 $m=2$ 且 n 为素数.

(2) 我们证明一个一般事实：对任意正整数 u, v，
$$\gcd(2^u-1,\ 2^v-1)=2^{\gcd(u,v)}-1.$$
证明如下：设 $d=\gcd(u,v)$. 对 $u\geq v$ 用带余除法写 $u=tv+r$（$t\geq 1$，$0\leq r<v$）. 用“辗转相减”法，
$$(2^u-1)-2^v(2^{u-v}-1)=2^{u-v}-1.$$

因此若某数同时整除 2^u-1 与 2^v-1，则也整除 $2^{u-v}-1$. 重复此过程（这与整数的欧几里得算法同步），最终得到它也整除 2^d-1. 反过来，由

$$2^u-1=(2^d)^{u/d}-1, \quad 2^v-1=(2^d)^{v/d}-1$$

可见 2^d-1 同时整除二者，于是最大公因数就是 2^d-1.

将此结论应用于 $u=p,\ v=q$ 两个不同的素数，因 $\gcd(p,q)=1$，得到

$$\gcd(M_p,M_q)=\gcd(2^p-1,2^q-1)=2^{\gcd(p,q)}-1=2^1-1=1.$$

从而 $(M_p,M_q)=1$. $\square$