代数学基础 2025秋 USTC

姓名：石泊远　　学号：PB25000051

2025 年 9 月 27 日

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

Proof. 借助辗转相除的思想，我们有

$$
\begin{aligned}
gcd\,(n!+1,(n+1)!+1) &= gcd\,(n!+1,(n+1)\,(n!+1)-n) = gcd\,(n!+1,n) \\
&= gcd\,(1,n) = 1
\end{aligned}
$$

Assignments 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

Proof. 用Euclid算法求963和657的最大公约数：

$$963 = 1 \times 657 + 306$$
$$657 = 2 \times 306 + 45$$
$$306 = 6 \times 45 + 36$$
$$45 = 1 \times 36 + 9$$
$$36 = 4 \times 9 + 0$$

由于最后一步的余数为0，因此$\gcd(963, 657) = 9$。
求方程$963x + 657y = gcd(963, 657)$的一组特解和所有整数解：
反着一步一步带入可得$22 * 659 - 15 * 963 = 9$，故此为一组正整数解
方程$963x + 657y = 9$的通解为：

$$x = -15 + \frac{657}{9}k = -15 + 73k$$
$$y = 22 - \frac{963}{9}k = 22 - 107k$$

其中k为任意整数。

Assignments 3.
设$a, b \in \mathbb{N}^*$，且$gcd\,(a, b) = 1$。证明当$n > ab - a - b$，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。

Proof. 我们先证后一个命题，即当$n = ab - a - b$时，方程无非负整数解。
假设存在一个非负整数解(x, y)，则整理得$a(x+1)+b(y+1) = ab$，而$gcd\,(a, b) = 1$，故可以得到$a \mid y + 1, b \mid x + 1$，一个基本的思路是设$y + 1 = ma, x + 1 = nb$,其中$m, n \in \mathbb{N}^*$ 则 $\Longrightarrow m + n = 1$，矛盾，也可以直接用整除导出不等关

系然后证出矛盾，故不存在正整数解

再证前一个命题，即当$n > ab - a - b$，方程

$$ax + by = n$$

存在非负整数解。

我们现在知道它存在整数解，先设为x_0与y_0，再扩增为一组通解

$$x = x_0 + bt$$

$$y = y_0 - at$$

同时研究两个变量是困难的，我们先考察一个单变量x，在$x \geq 0$，如果要同时让$y \geq 0$，让x尽可能小可以更容易的达成这一点

一定存在一个t，使得$x \in [0, b)$，并且我们可以认为它一定会成立，因为这是最小的，下面我们证明这一点。此时$y = \dfrac{n - ax}{b}$，又有$n - ax > ab - a - b - (ab - a) = -b \Longrightarrow y > -1$，而$y \in \mathbb{Z}$，故$y$为正整数

Assignments 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。

Proof. 我们先对问题进行分析，和素数有关的只有算术基本定理中涉及到过，所以考虑使用它

首先$1, 2..., n$是$n!$的因数，所以他们不可能是$n! - 1$的因数

如果$n! - 1$是质数，则n到$n!$间有质数

如果$n! - 1$不是质数，则n到$n!$间一定有它的质因子，所以则n到$n!$间有质数

就证明了n到$n!$之间至少有一个素数

我们取$n!$为新的n，记为n_1，可知n_1到$n_1!$间至少有一个质数，这个过程可以

一直进行下去，所以素数有无穷多个

弱哥德巴赫猜想，Betrend, Legendre

Assignments 5.
1.设m为正整数，证明：若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：若$m > n$，则$F_n \mid F_m - 2$
3.证明：若$m \neq n$，则$(F_m, F_n) = 1$。由此证明素数有无穷多个

Assignments 5's Remark. 费马数中的素数称为**费马素数**。例如

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

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

$$F_5 = 641 \times 6700417$$

不是素数。目前人们不知道除去前五个费马数外，是否还存在其他的费马素数

Proof. 1.若m不为2的方幂，则我们可以把它利用算术基本定理拆为$m = p \times q$，其中q是非一的奇数,p是二的幂次，则

$$2^m + 1 = 2^{pq} + 1 = (2^p + 1)(...)$$

括号内省略的部分显然大于1，则它不是素数，矛盾
2.

$$F_m - 2 = 2^{2^m} - 1 = \left(2^{2^{m-1}} + 1\right)\left(2^{2^{m-1}} - 1\right) = F_{m-1} \times (F_{m-1} - 2)$$

这是一个递推，继续下去有

$$F_m - 2 = F_{m-1} \times ... \times F_n \times (F_n - 2)$$

3.不妨设$m > n$，由2，我们有

$$(F_m, F_n) = (2, F_n) = 1$$

由于他们两两互素，所以每一个费马数的素因数都不一样，而费马数有无穷多个，故素数有无穷多个

Assignments 6.
1.设m, n都是大于1的整数，证明：若$m^n - 1$是素数，则$m = 2$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

$$(M_p, M_q) = 1$$

Assignments 6's Remark. 1644年，法国数学家梅森研究过形如$M_p = 2^p - 1$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**，网址：http://www.mersenne.org/default.php，是互联网上志愿者使用闲置计算机CPU来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梅森素数

$$M_74207281$$

，也是已知的第49个梅森素数。

Proof. 1.若$m > 2$，则$m^n - 1 = (m-1) \times (...) \equiv 0\,(mod\,m-1)$，括号内省略的部分显然大于1，矛盾，故$m = 2$
$m = 2$时，若n不为素数，则分解其为两个非一正整数的乘积$n = p \times q$，$2^n - 1 = 2^{pq} - 1 = (2^p - 1)\,(...)$，括号内省略的部分显然大于1，矛盾，故$n$是素数

2.不妨设$p > q$则

$$(M_p, M_q) = (2^p - 1, 2^q - 1) = \left(\sum_{i=0}^{p-1} 2^i, \sum_{j=0}^{q-1} 2^j \right) = (M_{p-q}, M_q)$$

类似于辗转相除，而$(p, q) = 1$，我们以x表示最后那个除出来的数，最后我们有$= (M_1, x) = 1$

Remark. 可能有些地方打错了，但是应该能被分辨出来我是打错的还是证错了