第一次作业

(2)

显然

$$a^3 - a = (a)(a+1)(a-1)$$

令k为整数，则

$$a = \begin{cases} 3k \\ 3k+1 \\ 3k+2 \end{cases}$$

如果$a = 3k$，则

$$3 \mid a$$

$$3 \mid a(a+1)(a-1)$$

同理，$a = 3k+1$和$a = 3k+2$时，

$$3 \mid a(a+1)(a-1)$$

也成立，从而得证。

(3)

若$k \in Z$，则一个奇整数a可以写成

$$a = 2k+1$$

它的平方为：

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

若k为奇数，即$k = 2p+1$，$p \in Z$

$$4k^2 + 4k = 16p^2 + 16p + 4 + 8p + 4 = 16p^2 + 24p + 8 = 8(p^2 + 3p + 1)$$

故

$$8 \mid 4k^2 + 4k$$

同理，k为偶数时，也有

$$8 \mid 4k^2 + 4k$$

故

$$a^2 \bmod 8 = ((4k^2 + 4k) \bmod 8) + 1 \bmod 8 = 1$$

这就是说，a^2具有$8k+1$的形式，得证。

(11)

用racket语言给出代码：

```
#lang racket

(define div
  (λ(x y)
    (= (modulo y x) 0)))

(define sieve
  (λ(now-stream max)
    (if (> (stream-first now-stream) max)
        empty-stream
        (stream-cons
         (stream-first now-stream)
         (sieve
          (stream-filter
           (λ(x) (not (div (stream-first now-stream) x)))
           (stream-rest now-stream))
          max)))))

(define number-from
  (λ(x)
    (stream-cons x
                 (number-from (+ x 1)))))

(stream->list (sieve (number-from 2) 500))
```

得到输出：

```
'(2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191
 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283
 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401
 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499)
```

(18)

$$(ABCDEFA)_{16} = (1010101111001101111011111010)_2$$

$$(DEFACEDA)_{16} = (11011110111110101100111011011010)_2$$

$$(9A0AB)_{16} = (10011010000010101011)_2$$

(28)

$$(55, 85) = 5$$

$$(202, 282) = 2$$

$$(666, 1414) = 2$$

$$(20785, 44350) = 5$$

(32)

1

$$1 = 0 \times 2 + 1 \times 1$$

$$1 = 1 \times 3 + -1 \times 2$$

$$1 = -1 \times 38 + 13 \times 3$$

$$1 = 13 \times 41 + -14 \times 38$$

$$1 = -14 \times 161 + 55 \times 41$$

$$1 = 55 \times 363 + -124 \times 161$$

$$1 = -124 \times 1613 + 551 \times 363$$

$$1 = 551 \times 3589 + -1226 \times 1613$$

$$1 = -1226 \times 1613 + 551 \times 3589$$

2

$$1 = 0 \times 3 + 1 \times 1$$

$$1 = 1 \times 4 + -1 \times 3$$

$$1 = -1 \times 115 + 29 \times 4$$

$$1 = 29 \times 119 + -30 \times 115$$

$$1 = -30 \times 353 + 89 \times 119$$

$$1 = 89 \times 472 + -119 \times 353$$

$$1 = -119 \times 825 + 208 \times 472$$

$$1 = 208 \times 2947 + -743 \times 825$$

$$1 = -743 \times 3772 + 951 \times 2947$$

$$1 = 951 \times 2947 + -743 \times 3772$$

3

$$1 = 0 \times 2 + 1 \times 1$$

$$1 = 1 \times 3 + -1 \times 2$$

$$1 = -1 \times 17 + 6 \times 3$$

$$1 = 6 \times 20 + -7 \times 17$$

$$1 = -7 \times 37 + 13 \times 20$$

$$1 = 13 \times 94 + -33 \times 37$$

$$1 = -33 \times 131 + 46 \times 94$$

$$1 = 46 \times 487 + -171 \times 131$$

$$1 = -171 \times 2079 + 730 \times 487$$

$$1 = 730 \times 2566 + -901 \times 2079$$

$$1 = -901 \times 17475 + 6136 \times 2566$$

$$1 = 6136 \times 20041 + -7037 \times 17475$$

$$1 = -7037 \times 37516 + 13173 \times 20041$$

$$1 = 13173 \times 20041 + -7037 \times 37516$$

4

$$1 = 0 \times 138 + 1 \times 1$$

$$1 = 1 \times 277 + -2 \times 138$$

$$1 = -2 \times 415 + 3 \times 277$$

$$1 = 3 \times 1107 + -8 \times 415$$

$$1 = -8 \times 822916 + 5947 \times 1107$$

$$1 = 5947 \times 1107 + -8 \times 822916$$

(33)

1

$$1 = 7 \times -2 + 10 \times -3 + 15 \times 3$$

2

$$7 = 70 \times 0 + 98 \times -1 + 105 \times 1$$

3

$$5 = 180 \times 0 + 330 \times 0 + 405 \times 51 + 590 \times -35$$

(37)

假设n不是合数，也就是说，n是质数。

$$n \mid a^2 - b^2$$

$$n \mid (a+b)(a-b)$$

由欧几里得引理，有：

$$(n \mid (a+b)) \quad or \quad (n \mid (a-b))$$

但由题设有：

$$not(n \mid (a+b)) \quad and \quad not(n \mid (a-b))$$

上下两式矛盾，所以假设不成立。这也就是说，n是合数，得证。

(49)

$$a^3 \mid b^2$$

表明

$$b^2 = k \cdot a^3 \ , \ k \in Z$$

那么，显然地：

$$b^2 = ak \cdot a^2 \ , \ k \in Z$$

这也就是说

$$a^2 | b^2$$

$$b^2 = k \cdot a^2$$

$$\frac{b^2}{a^2} = k \ , \ k \in N$$

由整数唯一分解定理：

$$\frac{p_1^{2t1} p_2^{2t2} p_3^{2t3} ... p_n^{2tn}}{q_1^{2k1} q_2^{2k2} q_3^{2k3} ... q_s^{2k_s}} = k \ , \ k \in N$$

其中p、q都是素数。

显然地，对$\forall i \in [1, \ s]$，有：

$$q_i^{2k_i} \mid b^2$$

由欧几里得引理，$\exists x \in [1, \ n]$，使得：

$$q_i^{2k_i} \mid p_x^{2t_x}$$

且由于p、q都是素数，$\nexists x$，使得当$j \neq i$时：

$$q_i^{2k_i} \mid p_x^{2t_x} \quad and \quad q_j^{2k_j} \mid p_x^{2t_x}$$

所以，只有相等的p_x与q_i才能使得$q_i^{2k_i} \mid p_x^{2t_x}$

把与$q_i^{2k_i}$对应的$p_x^{2t_x}$约去$q_i^{2k_i}$，得到

$$p_x^{2t_x - 2k_i}$$

这仍然是完全平方数，所有没有被约分的$p_x^{2t_x}$也是完全平方数，故他们的乘积，k，也是完全平方数。这就说明了：

$$\frac{b}{a} = y \ , \ y = \sqrt{k} \ , \ y \in N$$

即

$$a \mid b$$

(50)

1

$$[8, 60] = 120$$

2

$$[14, 18] = 126$$

3

$$[49, 77] = 539$$

4

$$[132, 253] = 3036$$

(53)

(i)

由于a，b，c是对称的，只需要证明在一种大小关系下该等式成立即可：

假设$a \le b \le c$

$$max(a, b, c) = a$$

$$a + b + c - min(a, b) - min(a, c) - min(b, c) + min(a, b, c) = a + b + c - b - c - c + c = a$$

故左式等于右式，原命题成立。

(ii)

对$\forall p$，p为质数的情况，设p^n整除a、b、c的最高次幂为α、β、γ。

定义

$$f(x, p) = max[n] \ , \ p^n \mid x$$

则由代数基本定理：

$$f([a, b, c], p) = max(\alpha, \beta, \gamma)$$

$$f((a, b, c), p) = min(\alpha, \beta, \gamma)$$

$$f(abc, p) = \alpha + \beta + \gamma$$

再由(i)中证明的式子，可以得出：

$$f([a,b,c],p)=f(\frac{(a,b,c)}{(a,b)(b,c)(a,c)},p)$$

由代数基本定理可知，若对于$\forall p, p\ is\ prime$，都有

$$f(a,p)=f(b,p)$$

则

$$a=b$$

所以

$$[a,b,c]=\frac{(a,b,c)}{(a,b)(b,c)(a,c)}$$

(60)

因为

$$1=-1\times 7+2\times 4$$

所以

$$100=-100\times 7+200\times 4$$

特解为

$$x=-100\ ,\ y=200$$

通解为

$$x=-100-4k\ ,\ y=200+7k\ ,\ k\in Z$$