1 习题 1.1 整除性

题目1. 设n是奇数，则$8 \mid n^2 - 1$

解答. If n is an odd number, then $n = 2k - 1$, where $k, k \in \mathbb{N}$. Therefore $n^2 - 1 = (2k-1)^2 - 1 = 4k^2 - 4k + 1 - 1$

$$= 4k^2 - 4k$$

$$= 4k(k-1)$$

For any $k > 1, k(k-1)$ will always be even, since an odd number multiplied by even number will always be even. Hence $k(k-1)$ will be divisible by 2, $2 \mid k(k-1)$. Therefore, $4k(k-1)$ has 4 as a factor, and we know

$$a \mid b \Rightarrow ac \mid bc$$

. Thus, it can be divisible by $2 \times 4 = 8$ as well.

题目2. 设$n \geq 3$是奇数，证明：

$$\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1}\right)(n-1)! \tag{*}$$

被n整除

解答. If n is an odd number, then $n = 2k + 1$, where $k, k \in \mathbb{N}$. We can rewrite the original equation

$$\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2k}\right)(2k)!$$

$$(2k)! + \frac{1}{2}(2k)! + \frac{1}{3}(2k)! + \cdots + \frac{1}{2k}(2k)! \tag{**}$$

And if we add the first and last term, second and second last, etc

$$(2k)! + \frac{1}{2k}(2k)! = (2k)!\frac{2k+1}{(2k)} \tag{1}$$

$$\frac{1}{2}(2k)! + \frac{1}{2k-1}(2k)! = (2k)!\frac{2k+1}{2(2k-1)} \tag{2}$$

$$\frac{1}{3}(2k)! + \frac{1}{2k-2}(2k)! = (2k)!\frac{2k+1}{3(2k-2)} \tag{3}$$

$$\cdots$$

$$\frac{1}{k}(2k)! + \frac{1}{k+1}(2k)! = (2k)!\frac{2k+1}{k(k+1)} \tag{4}$$

We know that (1)(2)(3) . . . (k) all have $2k+1$ as a factor, then we know that (1)+(2)+(3)+. . . (k) can also be factored Thus, we know that $2k + 1 \mid (**)$. Therefore, $n \mid (*)$ is true.

题目3. 设m和n是正整数$m \geq 3$，证明$2^m - 1 \nmid 2^n + 1$.

解答. Proof by contradiction. Let us assume that $2^m - 1 \mid 2^n + 1$. That means $2^n - 1 > 2^m + 1$, $m \geq 3$, $n \geq m$.
Thus there exists $a \in \mathbb{Z}$, where $n = m - a$.

$$2^n + 1 = 2^{m+a} + 1 = 2^m 2^a + 1 = 2^m 2^a + 1 + 2^a - 2^a = 2^a(2^m - 1) + 2^a + 1$$

If it is divisible, then

$$\Rightarrow 2^a + 1 \mid 2^m - 1$$

Let $m > a, m = a + x$
And repeat . . .
We find that $2^x + 1 < 2^m - 1$ and the left hand size is always smaller. Which means that there exists decimal, but from $2^a + \ldots$ are all integers, which is a contradiction. Therefore $2^m - 1 \nmid 2^n + 1$

题目4. 设q是大于1的整数，证明:

解答. 1. If we use the division algorithm, then there exists integer k such that

$$n = q_1 b + a_0, 0 \leq a_0 \leq b - 1, q_1 \geq b$$

$$q_1 = q_2 b + a_1, 0 \leq a_1 \leq b - 1, q_2 \geq b$$

$$\ldots$$

$$q_{k-1} = q_k b + a_{k-1}, 0 \leq a_{k-1} \leq b - 1, 0 < q_k \leq b - 1$$

And thus since a_i and q_i are both uniquely determined, $q_k = a_k$, where $0 < a_k \leq b - 1$

$$n = q_1 b + a_0 = (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0$$

$$= (q_3 b + a_2)b^2 + a_1 b + a_0 = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

$$= \ldots$$

$$= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

2.

题目5. 设$a_1, \ldots, a_n$，为实数$(n \geq 2)$,证明:

解答. Since we know that $\{a\} = a - [a]$ or $[a] = a - \{a\}$ or $a = [a] + \{a\}$

$$[a_1] + [a_2] + \cdots + [a_n] = (a_1 + \cdots + a_n) - (\{a_1\} + \cdots + \{a_n\})$$

$$[a_1 + \cdots + a_n] = (a_1 + \cdots + a_n) - \{a_1 + \cdots + a_n\}$$

$$\{a_1\} + \cdots + \{a_n\} \geq \{a_1 + \cdots + a_n\}$$

$$\Rightarrow [a_1] + [a_2] + \cdots + [a_n] \leq [a_1 + \cdots + a_n]$$

We also know that $\{a_1\} + \cdots + \{a_n\} < n$ since each element is less than 1. And we know by definition that

$$\{a_1 + \cdots + a_n\} < 1$$

题目11. 设n是正整数$n \geq 2$，如果n没有小于或等于$\sqrt{n}$素数因子，则n是素数

解答. Every integer $n > 1$ can be uniquely expressed as a product of primes. So, n is composite, with least prime divisor p_0, then $n = mp_0$ with $m > 1$ and no prime divisor of m less than p_0. Therefore, $m \geq p_0$ and so $n \geq p_0^2$. If n must have at least one prime divisor when $\leq \sqrt{n}$ whenever n is composite. Thus, if n has no prime divisor $\leq \sqrt{n}$ and $n > 1$, then n must be prime.

题目12. 对于每个整数$n \geq 3$，n和$n!$，之间必有素数，由此证明素数有无限多

解答. The base case or this problem would be when $n = 3$, such that $3 < x < 3!$, where $x = 5$
Let p be any prime number that divides $n! - 1$
Since $p|n! - 1$, p does not divide $n!$ And it shows that p cannot be equal to or less than n since $n! = n \times (n-1)!$, if it does, p could divide $n!$, therefore

$$p > n$$

Also, p divides $n! - 1$ so, p is less than or equal to $n! - 1$, and thus

$$n < p < n!$$

There is a prime between n and $n!$

2 习题1.2 最大归约和最小公倍数

题目1. 设n是正整数，证明$\frac{21n+4}{14n+3}$是既约分数

解答. An irreducible fraction is one such that the numerator and denominator are integers that have no common divisors other than 1. In other words, a fraction a/b is irreducible iff a and b are coprime, $GCD(a, b) = 1$ Using Euclid's Algorithm, and the divisibility algorithm $a = qb + r, 0 \leq r \leq b$

$$GCD(21n + 4, 14n + 3) = 21n + 4 = 1(14n + 3) + 7n + 1$$

$$GCD(14n + 3, 7n + 1) = 2(7n + 1) + 1$$

$$GCD(7n + 1, 1) = 1$$

Thus we can say that $\frac{21n+4}{14n+3}$ is an irreducible fraction.

题目2. 设m, n为正整数，m为奇数，证明

$$(2^m - 1, 2^n + 1) = 1$$

解答. Using the result we have obtained from question 3, we can start of with

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$$

Therefore we can conclude that

$$\left(a^m - 1, a^{2n} - 1\right) = a^{(m,2n)} - 1$$

However, since m is odd, by Euclid's lemma, we know that $(m, 2n) = (m, n)$, if and only if m is odd , therefore

$$(2^n - 1, 2^n + 1) = (2^n - 1, 2) \mid 2$$

And if $2^{(m,2n)} - 1$ is odd, it implies, $(2^{(m,2n)} - 1, 2^n + 1) = 1$

$$\Rightarrow (2^m - 1, 2^n + 1) = 1$$

题目3. 设m, n, a均为正整数，$a \geq 2$，证明：

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$$

解答.

Method 1: Assume $a, b \in \mathbb{Z}$

$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1) = (2^a - 1)\sum_{i=0}^{b-1}(2^a)^i$$

$$\Rightarrow 2^a - 1 \mid 2^{ab} - 1$$

So if we let value $d = (m, n)$, we can also rewrite it as

$$2^m - 1 = (2^d)^{\frac{m}{d}} - 1 = (2^d - 1)\sum_{i=0}^{\frac{m}{d}-1}(2^d)^i$$

$$\Rightarrow 2^d - 1 \mid 2^m - 1$$

$$\Rightarrow 2^d - 1 \mid 2^n - 1$$

And we get that

$$\Rightarrow 2^{(m,n)} - 1 \mid (2^m - 1, 2^n - 1)$$

There must exist a, b, such that $(m, n) = am - bn$ and Let $M = (2^m - 1, 2^n - 1)$, we get

$$M \mid 2^m - 1 \Rightarrow M \mid 2^{am} - 1$$

$$M \mid 2^n - 1 \Rightarrow M \mid 2^{bn} - 1$$

Then

$$\Rightarrow M \mid ((2^{am} - 1) - (2^{bn} - 1))$$

$$M \mid 2^{bn} * (2^{am-bn} - 1)$$

Subsituting, $(m, n) = am - bn$ back into the equation,

$$\Rightarrow M \mid 2^{(m,n)} - 1$$

$$\therefore (2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$$

This works for base 2, as well as for any $a \geq 2$.

解答.

Method 2

Set $d = (m, n)$, $sd = m, td = n$. Then

$$a^m - 1 = (a^d)^s - 1$$

and like before

$$a^d - 1 \mid (a^d)^s - 1$$

This goes for $a^n - 1$ as well

$$a^d - 1 \mid (a^d)^t - 1$$

Therefore

$$\Rightarrow a^d - 1 \mid (a^m - 1, a^n - 1)$$

Now, by the Bachet-Bezout Theorem, there are integers x, y with $(m, n) = mx + ny = d$ However, x and y must have opposite signs. They can't both be negative, or d would be negative. They both cannot be positive either or else $d \geq n + m$ when the conditions given were $d \leq m, d \leq n$. So if we assume $x > 0, y \leq 0$, we get $(m, n) = mx - ny = d$. Setting $t = (a^m - 1, a^n - 1)$, we get

$$t \mid (a^{mx} - 1)$$

$$t \mid (a^{-ny} - 1)$$

$$\Rightarrow t \mid ((2^{mx} - 1) - a^d(2^{-ny} - 1)) = a^d - 1$$

And the assertion is established

解答.

Method 3

This can be mimicked by an subtractive Euclidean algorithm $(n, m) = (n-m, m)$. For example

$$(f_5, f_2) = (f_3, f_2) = (f_1, f_2) = (f_1, f_1) = (f_1, f_0) = f_1 = f_{(5,2)}$$

such as

$$(5, 2) = (3, 2) = (1, 2) = (1, 1) = (1, 0) = 1$$

because

$$f_n := a^n - 1 = a^{n-m}(a^m - 1) + a^{n-m} - 1$$

$$\Rightarrow f_n = f_{n-m} + kf_m, k \in Z$$

By induction, $n+m$, thereom obviously true for $n=m$ or $n=0$ or $m=0$. So we may assume $n>m>0$, and we know that $(f_n, f_m) = (f_{n-m}, f_m)$ because of Euclid and the Since $(n-m)+m < n+m$, induction yields

$$(f_{n-m}, f_m) = f_{(n-m,m)} = f_{(n,m)}$$

And if we apply it to above, we know that

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$$

This is known as a strong divisibility sequence