# MATH 324 Summer 2006
# Elementary Number Theory
# Solutions to Assignment 1
# Due: Wednesday July 19, 2006

**Department of Mathematical and Statistical Sciences**
**University of Alberta**

**Question 1. [p 13. #5]**

Use the well–ordering property to show that $\sqrt{3}$ is irrational.

SOLUTION: Since $1 < 3 < 4$, it follows from the order properties of the integers that $1 < \sqrt{3} < 2$.

Now suppose that $\sqrt{3}$ is rational, then there exist positive integers $m$ and $n$ such that

$$\sqrt{3} = \frac{m}{n}.$$

Let $S$ be the set of all positive integers $n$ such that $\sqrt{3} = \dfrac{m}{n}$ for some positive integer $m$, then $S \neq \emptyset$, and by the well–ordering property, $S$ has a smallest element, say $b$, and therefore $\sqrt{3} = \dfrac{a}{b}$ for some positive integer $a$.

Now, since $1 < \dfrac{a}{b} < 2$, then $b < a < 2b$, that is, $0 < a - b < b$, and $a - b$ is a positive integer less than $b$.
But, $\sqrt{3} = \dfrac{a}{b}$ implies that $3b^2 = a^2$, so that $3b^2 - ab = a^2 - ab$, that is, $b(3b - a) = a(a - b)$, and since $a$, $b$, and $a - b$ are all positive, then $3b - a > 0$, and

$$\sqrt{3} = \frac{a}{b} = \frac{3b - a}{a - b}.$$

Therefore, we have written $\sqrt{3}$ as a ratio of two integers with positive integer denominator $a - b$ which is less than $b$. This contradicts the choice of $b$, however. Therefore, $\sqrt{3}$ is irrational.

**Question 2. [p 13. #19]**

Show that

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor \sqrt{x} \rfloor$$

whenever $x$ is a nonnegative real number.

SOLUTION: Let $x$ be a nonnegative real number and let $m = \lfloor \sqrt{x} \rfloor$, so that

$$m \leq \sqrt{x} < m + 1.$$

Since $m \geq 0$, from the order properties of the nonnegative real numbers we have

$$m^2 \leq x < (m + 1)^2,$$

and from the properties of the greatest integer function we have

$$m^2 \leq \lfloor x \rfloor < (m + 1)^2.$$

Again, from the order properties of the nonnegative real numbers, this implies that

$$m \leq \sqrt{\lfloor x \rfloor} < m + 1,$$

which implies that $m = \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$, so that $\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \lfloor \sqrt{x} \rfloor$.

**Question 3. [p 21. #5]**

Find and prove a formula for

$$\sum_{k=1}^{n} \left\lfloor \sqrt{k} \right\rfloor$$

in terms of $n$ and $\lfloor \sqrt{n} \rfloor$.

Solution: Note that if $a_1, a_2, \cdots, a_n$ are nonnegative integers, and we let

$f(1)$ denote the number of them that are greater than or equal to 1,

$f(2)$ denote the number of them that are greater than or equal to 2,

$f(3)$ denote the number of them that are greater than or equal to 3,

$\vdots$

then

$$a_1 + a_2 + \cdots + a_n = f(1) + f(2) + f(3) + \cdots$$

since $a_k$ contributes 1 to each of the numbers $f(1), f(2), \cdots, f(a_k)$.

For this particular problem, we take $a_k = \left\lfloor \sqrt{k} \right\rfloor$ for $1 \leq k \leq n$, and note that:

- $f(1)$ is the number of $a_k$'s such that $\sqrt{k} \geq 1$, that is, the number of $k$'s with $1 \leq k \leq n$ such that $k \geq 1$, so that $f(1) = n$.
- $f(2)$ is the number of $a_k$'s such that $\sqrt{k} \geq 2$, that is, the number of $k$'s with $1 \leq k \leq n$ such that $k \geq 2^2 = 4$, so that $f(2) = n - 3$.
- $f(3)$ is the number of $a_k$'s such that $\sqrt{k} \geq 3$, that is, the number of $k$'s with $1 \leq k \leq n$ such that $k \geq 3^2 = 9$, so that $f(2) = n - 8$.

  $\vdots$

In general, if $1 \leq m \leq \lfloor \sqrt{n} \rfloor$, then

- $f(m)$ is the number of $k$'s such that $\sqrt{k} \geq m$, that is, the number of $k$'s with $1 \leq k \leq n$ such that $k \geq m^2$, so that $f(m) = n - (m^2 - 1)$.

Therefore,

$$\sum_{k=1}^{n} \left\lfloor \sqrt{k} \right\rfloor = \sum_{m=1}^{\infty} f(m) = \sum_{m=1}^{\lfloor \sqrt{n} \rfloor} \left[ n - (m^2 - 1) \right],$$

so that

$$\sum_{k=1}^{n} \left\lfloor \sqrt{k} \right\rfloor = (n+1) \lfloor \sqrt{n} \rfloor - \sum_{m=1}^{\lfloor \sqrt{n} \rfloor} m^2 = (n+1) \lfloor \sqrt{n} \rfloor - \frac{\lfloor \sqrt{n} \rfloor (\lfloor \sqrt{n} \rfloor + 1)(2 \lfloor \sqrt{n} \rfloor + 1)}{6}.$$

An easy induction argument shows that this is correct, the details are omitted.

**Question 4. [p 27. #5]**

Conjecture a formula for $A^n$ where $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Prove your conjecture using mathematical induction.

Solution: For small values of $n$ we have

$$\begin{aligned}
A^1 &= A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
A^2 &= A \cdot A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
A^3 &= A \cdot A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \\
A^4 &= A \cdot A^3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \\
A^5 &= A \cdot A^4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \\
&\vdots
\end{aligned}$$

and it appears that

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \tag{$*$}$$

for all positive integers $n$. We prove this conjecture using mathematical induction.

*Base Case*: We have seen above that $(*)$ is true for $n = 1, 2, 3, 4, 5$.

*Inductive Step*: Let $n$ be an arbitrary positive integer, with $n \geq 1$, and suppose that $(*)$ is true for $n$, then

$$A^{n+1} = A \cdot A^n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix},$$

and $(*)$ is also true for $n+1$.

Therefore, from the principle of mathematical induction, $(*)$ is true for all integers $n \geq 1$.

**Question 5. [p 27. #8]**

Use mathematical induction to prove that

$$\sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} \tag{$**$}$$

for every positive integer $n$.

Solution: We prove that $(**)$ is true using the principle of mathematical induction:

*Base Case*: For $n = 1$,

$$\sum_{k=1}^{1} k^3 = 1^3 = \frac{1^2(1+1)^2}{4}$$

so that $(**)$ is true for $n = 1$.

*Inductive Step*: Now suppose that $(**)$ is true for some $n \geq 1$, then

$$\begin{aligned}\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 &= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\ &= \frac{(n+1)^2}{4}\left[n^2 + 4(n+1)\right] \\ &= \frac{(n+1)^2(n+2)^2}{4}\end{aligned}$$

so that $(**)$ is true for $n+1$. Therefore, by the principle of mathematical induction, $(**)$ is true for all $n \geq 1$.

**Question 6. [p 28. #20]**

Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.

SOLUTION: For $n = 4$ we have $2^4 = 16 < 24 = 4!$, and the result is true for the base case $n = 4$.

Assuming the result is true for some integer $n \geq 4$, we have

$$(n+1)! = (n+1) \cdot n! > (n+1) \cdot 2^n > 2 \cdot 2^n = 2^{n+1}$$

since $n \geq 4$. Therefore the result is also true for $n + 1$.

By the principle of mathematical induction, $2^n < n!$ for all $n \geq 4$.

**Question 7. [p 34. #16]**

Prove that

$$f_1 f_2 + f_2 f_3 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2 \qquad (***)$$

if $n$ is a positive integer.

SOLUTION: We will prove $(***)$ using the principle of mathematical induction.

*Base Case*: For $n = 1$, we have $f_1 f_2 = 1 \cdot 1 = f_2^2$, and $(***)$ holds for $n = 1$.

*Inductive Step*: Assume that $(***)$ is true for some $n \geq 1$, then from the inductive hypothesis we have

$$\begin{aligned}f_1 f_2 + f_2 f_3 + \cdots + f_{2n-1} f_{2n} &+ f_{2n} f_{2n+1} + f_{2n+1} f_{2n+2} \\ &= f_{2n}^2 + f_{2n} f_{2n+1} + f_{2n+1} f_{2n+2} \\ &= f_{2n}(f_{2n} + f_{2n+1}) + f_{2n+1} f_{2n+2} \\ &= f_{2n} f_{2n+2} + f_{2n+1} f_{2n+2} \\ &= (f_{2n} + f_{2n+1}) f_{2n+2} \\ &= f_{2n+2}^2,\end{aligned}$$

and $(***)$ is true for $n + 1$ also. By the principle of mathematical induction, $(***)$ is true for all integers $n \geq 1$.

We can also give a direct proof using Cassini's identity. For $k \geq 1$, we have

$$f_k^2 = (f_{k+1} - f_{k-1})^2 = f_{k+1}^2 - 2f_{k+1}f_{k-1} + f_{k-1}^2,$$

so that

$$\begin{aligned} f_{k+1}^2 - f_k^2 &= 2f_{k+1}f_{k-1} - f_{k-1}^2 \\ &= f_{k+1}f_{k-1} + f_{k-1}(f_{k+1} - f_{k-1}) \\ &= f_{k+1}f_{k-1} + f_{k-1}f_k \\ &= (-1)^k + f_k^2 + f_{k-1}f_k \\ &= (-1)^k + f_k(f_k + f_{k-1}) \\ &= (-1)^k + f_k f_{k+1}. \end{aligned}$$

Note that this also holds for $k = 0$, so that

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

for all $k \geq 0$, and summing over $k$, we have

$$\sum_{k=0}^{2n-1} \left(f_{k+1}^2 - f_k^2\right) = \sum_{k=0}^{2n-1} (-1)^k + \sum_{k=0}^{2n-1} f_k f_{k+1}.$$

The sum on the left telescopes to $f_{2n}^2$ and the first sum on the right is 0, so that

$$f_{2n}^2 = \sum_{k=0}^{2n-1} f_k f_{k+1}$$

for all $n \geq 1$.

**Question 8. [p 35. #31]**

Show that $f_n \leq \alpha^{n-1}$ for every integer $n$ with $n \geq 2$, where $\alpha = (1 + \sqrt{5})/2$.

Solution: We will use the strong principle of mathematical induction to show that

$$f_n \leq \alpha^{n-1} \qquad (****)$$

for all $n \geq 2$.

Note first that

$$\alpha^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2} = 1 + \alpha.$$

*Base Case*: For $n = 2$ we have $f_2 = 1 < \alpha^{2-1} = \alpha$, since $\sqrt{5} > 1$. For $n = 3$ we have $f_3 = 2$ and $f_3 = 2 < 1 + \alpha = \alpha^2 = \alpha^{3-1}$. Therefore $(****)$ is true for both $n = 2$ and $n = 3$.

*Inductive Step*: Now let $n$ be a positive integer with $n \geq 3$, and assume that $(****)$ is true for all integers $k$ with $3 \leq k \leq n$, then from the inductive hypothesis

$$f_{n+1} = f_n + f_{n-1} \leq \alpha^{n-1} + \alpha^{n-2} = \alpha^{n-2}(1+\alpha) = \alpha^{n-2}\alpha^2 = \alpha^n,$$

so that $(****)$ is true for $n+1$ also. By the strong principle of mathematical induction $(****)$ is true for all integers $n \geq 2$.

**Question 9. [p 35. #33]**

Prove that whenever $n$ is a nonnegative integer,

$$\sum_{k=1}^{n} \binom{n}{k} f_k = f_{2n},$$

where $f_k$ is the $k$th Fibonacci number.

SOLUTION: We use Binet's formula for the Fibonacci numbers and the binomial theorem. First note that

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1-\sqrt{5}}{2}$$

are the distinct real roots of the quadratic $x^2 = 1 + x$, and Binet's formula for $f_k$ is

$$f_k = \frac{1}{\sqrt{5}} \left[\alpha^k - \beta^k\right].$$

Since $f_0 = 0$, then from the binomial theorem we have

$$\begin{aligned}
\sum_{k=1}^{n} \binom{n}{k} f_k &= \sum_{k=0}^{n} \binom{n}{k} f_k \\
&= \frac{1}{\sqrt{5}} \sum_{k=0}^{n} \binom{n}{k} \alpha^k - \frac{1}{\sqrt{5}} \sum_{k=0}^{n} \binom{n}{k} \beta^k \\
&= \frac{1}{\sqrt{5}} (1+\alpha)^n - \frac{1}{\sqrt{5}} (1+\beta)^n \\
&= \frac{1}{\sqrt{5}} \left[(\alpha^2)^n - (\beta^2)^n\right] \\
&= \frac{1}{\sqrt{5}} \left[\alpha^{2n} - \beta^{2n}\right] \\
&= f_{2n}
\end{aligned}$$

for all $n \geq 0$.

**Question 10. [p 40. #21]**

Show that the number of positive integers less than or equal to $x$, where $x$ is a positive real number, that are divisible by the positive integer $d$ equals $\lfloor x/d \rfloor$.

SOLUTION:

SOLUTION: Let $k$ be the number of positive integers less than or equal to $x$ that are divisible by $d$, then

$$0 < 1 \cdot d < 2 \cdot d < 3 \cdot d < \cdots < k \cdot d \leq x$$

but $(k+1) \cdot d > x$, that is,

$$k \cdot d \leq x < (k+1) \cdot d,$$

so that

$$k \leq \frac{x}{d} < k+1,$$

and $k = \left\lfloor \frac{x}{d} \right\rfloor$.

**Question 11. [p 41. #34]**

Use mathematical induction to show that $n^7 - n$ is divisible by 7 for every positive integer $n$.

SOLUTION: For $n = 1$, $n^7 - n = 0$, and $7 \mid 0$.

Now assume that $7 \mid n^7 - n$, for some integer $n \geq 1$, then

$$(n+1)^7 - (n+1) = n^7 + 7n^6 + 21n^5 + 35n^4 + 35n^3 + 21n^2 + 7n + 1 - n - 1,$$

that is,

$$(n+1)^7 - (n+1) = n^7 - n + (7n^6 + 21n^5 + 35n^4 + 35n^3 + 21n^2 + 7n),$$

so that $7 \mid (n+1)^7 - (n+1)$. Therefore, by the principle of mathematical induction, $7 \mid n^7 - n$ for all positive integers $n$.

**Question 12. [p 41. #36]**

Let $f_n$ denote the $n$th Fibonacci number. Show that $f_n$ is even if and only if $n$ is divisible by 3.

SOLUTION: For any integer $n \geq 0$, we have

$$f_{n+3} = f_{n+2} + f_{n+1} = f_{n+1} + f_n + f_{n+1} = 2f_{n+1} + f_n,$$

so that $f_{n+3}$ is even if and only if $f_n$ is even.

Now, since $f_0 = 0$ is even, the above implies that $f_{3n}$ is even for all $n \geq 0$. However, since $f_1 = 1$ and $f_2 = 1$ are odd, then $f_{3n+1}$ and $f_{3n+2}$ are odd for all $n \geq 0$.

Therefore $f_n$ is even if and only if $n$ is divisible by 3.

**Question 13. [p 41 #40]**

Show that

$$f_{n+m} = f_m f_{n+1} + f_{m-1} f_n$$

whenever $m$ and $n$ are positive integers with $m > 1$. Use this result to show that $f_n \mid f_m$ when $m$ and $n$ are positive integers with $n \mid m$.

SOLUTION: Letting $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, an easy induction argument shows that

$$A^k = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix}$$

for all integers $k \geq 1$.

Therefore,

$$A^{m+m} = \begin{pmatrix} f_{m+n+1} & f_{m+n} \\ f_{m+n} & f_{m+n-1} \end{pmatrix}$$

for all positive integers $m$ and $n$. On the other hand, $A^{m+n} = A^m \cdot A^n$, so that

$$A^{m+n} = \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = \begin{pmatrix} f_{m+1}f_{n+1} + f_m f_n & f_{m+1}f_n + f_m f_{n-1} \\ f_m f_{n+1} + f_{m-1}f_n & f_m f_n + f_{m-1}f_{n-1} \end{pmatrix}$$

and equating the entries in the second row and the first column, we have

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n.$$

Now note that if $d$ is a positive common divisor of $f_n$ and $f_{n+1}$, since $f_{n-1} = f_{n+1} - f_n$, then $d$ is a positive divisor of $f_{n-1}$ also. An easy induction argument then shows that $d$ must be a positive divisor of $f_2 = 1$, that is, $d = 1$. Therefore any two consecutive Fibonacci numbers must be relatively prime.

If $m$ and $n$ are positive integers with $m > 1$, then $f_n \,\big|\, f_{m+n}$ if and only if $f_n \,\big|\, f_m f_{n+1}$, and since $f_n$ and $f_{n+1}$ are relatively prime, then $f_n \,\big|\, f_{m+n}$ if and only if $f_n \,\big|\, f_m$.

We will show by induction that whenever $n \,\big|\, m$, so that $m = k \cdot n$ for some integer $k \geq 1$, then $f_n \,\big|\, f_m$.

*Base Case*: For $k = 1$, we have $f_n \,\big|\, f_{1\cdot n}$ and the result is true for $k = 1$.

*Inductive Step*: Assume now that $m = k \cdot n$ for some integer $k \geq 1$, and that $f_n \,\big|\, f_{k\cdot n}$, that is, $f_n \,\big|\, f_m$, from the above, this implies that

$$f_n \,\big|\, f_{m+n},$$

that is, $f_n \,\big|\, f_{(k+1)n}$, and so the result is true for $k + 1$ also.

Therefore by the principle of mathematical induction, $f_n \,\big|\, f_m$ whenever $m$ and $n$ are positive integers such that $n \,\big|\, m$.

**Question 14. [p 41. #45]**

Show that $\lfloor (2 + \sqrt{3})^n \rfloor$ is odd whenever $n$ is a nonnegative integer.

SOLUTION: For any $n \geq 0$,

$$\begin{aligned}(2+\sqrt{3})^n + (2-\sqrt{3})^n &= \sum_{k=0}^{n} \binom{n}{k} 2^k \cdot (\sqrt{3})^{n-k} + \sum_{k=0}^{n} \binom{n}{k} 2^k (-1)^{n-k} (\sqrt{3})^{n-k} \\ &= 2 \cdot \sum_{\substack{k=0 \\ n-k \text{ even}}}^{n} \binom{n}{k} 2^k \cdot (\sqrt{3})^{n-k},\end{aligned}$$

so that $(2+\sqrt{3})^n + (2-\sqrt{3})^n$ is an *even integer* for $n \geq 0$.

For $n = 0$, $(2+\sqrt{3})^0 = 1$, so that $\lfloor (2+\sqrt{3})^0 \rfloor = 1$ is odd.

For $n \geq 1$, let $N = (2+\sqrt{3})^n + (2-\sqrt{3})^n$, so that $N$ is an even integer. Since $0 < 2 - \sqrt{3} < 1$, then $0 < (2-\sqrt{3})^n < 1$, for all $n \geq 1$, and

$$(2+\sqrt{3})^n = N - (2-\sqrt{3})^n = N - 1 + 1 - (2-\sqrt{3})^n,$$

where $0 \leq 1 - (2-\sqrt{3})^n < 1$. Therefore, $\lfloor (2+\sqrt{3})^n \rfloor = N - 1$ is an odd integer for all $n \geq 0$.

**Question 15. [p 50. #29]**

A **Cantor expansion** of a positive integer $n$ is a sum

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1!,$$

where each $a_k$ is an integer with $0 \le a_k \le k$ and $a_m \ne 0$.

Show that every positive integer has a unique Cantor expansion. (*Hint*: For each positive integer $n$ there is a positive integer $m$ such that $m! \le n < (m+1)!$. For $a_m$, take the quotient from the division algorithm when $n$ is divided by $m!$, then iterate.)

SOLUTION:

*Existence*: Following the hint, if $n > 0$, from the well-ordering property, there is a unique positive integer $m$ such that

$$m! \le n < (m+1)!.$$

Now we use the division algorithm to divide $n$ by $m!$ to get

$$n = a_m \cdot m! + r_m$$

where the quotient $a_m$ satisfies $0 \le a_m \le m$, and the remainder $r_m$ satisfies

$$0 \le r_m < m!.$$

We use the division algorithm again to divide $r_m$ by $(m-1)!$ to get

$$r_m = (m-1)! \cdot a_{m-1} + r_{m-1}$$

where the quotient $a_{m-1}$ satisfies $0 \le a_{m-1} \le m-1$, and the remainder $r_{m-1}$ satisfies

$$0 \le r_{m-1} < (m-1)!.$$

Next use the division algorithm to divide $r_{m-1}$ by $(m-2)!$ to get

$$r_{m-1} = (m-2)! \cdot a_{m-2} + r_{m-2}$$

where the quotient $a_{m-2}$ satisfies $0 \le a_{m-2} \le m-2$, and the remainder $r_{m-2}$ satisfies

$$0 \le r_{m-2} < (m-2)!.$$

By the well-ordering property of the nonnegative integers, this process must stop after at most $m$ steps, and the result is the representation

$$n = a_m \cdot m! + a_{m-1} \cdot (m-1)! + \cdots + a_2 \cdot 2! + a_1 \cdot 1!,$$

where each $a_k$ is an integer with $0 \le a_k \le k$ and $a_m \ne 0$.

*Uniqueness*: Suppose that $n$ is a positive integer which has two different Cantor expansions, say

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1! = b_m m! + b_{m-1}(m-1)! + \cdots + b_2 2! + b_1 1!, \qquad (+)$$

where $a_k$ and $b_k$ are integers with $0 \le a_k, b_k \le k$ for $k = 1, 2, \ldots, m$.

Let $k_0$ be the largest positive integer such that $a_{k_0} \neq b_{k_0}$, and assume that $a_{k_0} > b_{k_0}$, since these are integers, this implies that $a_{k_0} \geq b_{k_0} + 1$. Cancelling terms that are equal in (+), we have

$$a_{k_0} k_0! + a_{k_0-1}(k_0 - 1)! + \cdots + a_2 2! + a_1 1! = b_{k_0} k_0! + b_{k_0-1}(k_0 - 1)! + \cdots + b_2 2! + b_1 1!,$$

and using the identity

$$1 \cdot 1! + 2 \cdot 2! + \cdots + k_0 \cdot k_0! = (k_0 + 1)! - 1,$$

we have

$$\begin{aligned} b_{k_0} k_0! + b_{k_0-1}(k_0 - 1)! + \cdots + b_2 2! + b_1 1! &\leq b_{k_0} k_0! + (k_0 - 1) \cdot (k_0 - 1)! + \cdots + 2 \cdot 2! + 1 \cdot 1! \\ &= b_{k_0} k_0! + k_0! - 1 \\ &= (b_{k_0} + 1) k_0! - 1 \\ &< a_{k_0} k_0!, \end{aligned}$$

which is a contradiction. Therefore the Cantor expansion of a positive integer is unique.

This representation of a positive integer $n$ is also called the **factorial representation** of $n$ and the $a_i$'s are called the **factorial digits** of $n$.