$\mathbb{ITYM}$ 2021 - Problem 6: Binomial Coefficients and Prime Numbers

Presented by Philémon
France

Compoundness : definitions

An integer $n \geqslant 2$ is *S-compound* if for each $1 \leqslant k \leqslant n-1$, $\binom{n}{k}$ is divisible by one number from S (a set of integers).

An integer n is *ℓ-compound* if there exists a set S of ℓ prime numbers s.t. n is S-compound.

Compoundness : definitions

An integer $n \geqslant 2$ is *S-compound* if for each $1 \leqslant k \leqslant n-1$, $\binom{n}{k}$ is divisible by one number from S (a set of integers).

An integer n is *ℓ-compound* if there exists a set S of ℓ prime numbers s.t. n is S-compound.

Example of S-compoundness

$n = 0:$	1							
$n = 1:$	1	1						
$n = 2:$	1	2	1					
$n = 3:$	1	3	3	1				
$n = 4:$	1	4	6	4	1			
$n = 5:$	1	5	10	10	5	1		
$n = 6:$	1	6	15	20	15	6	1	
$n = 7:$	1	7	21	35	35	21	7	1

Example with $n = 6$ and $S = \{3, 5\}$: n is S-compound

1. a) $\{p\}$-compoundness with p a prime

Useful tool : **Lucas's Theorem**

Let p a prime number. If $n = \overline{a_\ell\ a_{\ell-1}\ \ldots\ a_0}^p$ and $k = \overline{b_\ell\ b_{\ell-1}\ \ldots\ b_0}^p$ then

$$\binom{n}{k} \equiv \prod_{i=0}^{\ell} \binom{a_i}{b_i} \mod p$$

1. a) $\{p\}$-compoundness with p a prime

Useful tool : **Lucas's Theorem**
Let p a prime number. If $n = \overline{a_\ell \; a_{\ell-1} \; \dots \; a_0}^p$ and $k = \overline{b_\ell \; b_{\ell-1} \; \dots \; b_0}^p$ then

$$\binom{n}{k} \equiv \prod_{i=0}^{\ell} \binom{a_i}{b_i} \mod p$$

1. a) $\{p\}$-compoundness with p a prime

Claim :
The only $\{p\}$-compound integers are the powers of p.
Sketch of proof :
▷ we note $n = \overline{a_\ell \; a_{\ell-1} \; \dots \; a_0}^p$ and we use Lucas's Theorem with specific k's to show that we must have $a_0 = a_1 = \dots = a_{\ell-1} = 0$ and $a_\ell = 1$, which precisely means that $n = p^\ell$
▷ if $n = p^\ell$, then for each $1 \leqslant k \leqslant n-1$, there exists a non-zero digit b_i of k in base p and using once again Lucas's Theorem gives $\binom{p^\ell}{k} \equiv \binom{1}{0} \prod_{i=0}^{\ell-1} \binom{0}{b_i} \equiv 0 \mod p$ and show the equivalence. ■

1. a) $\{p\}$-compoundness with p a prime

Claim :
The only $\{p\}$-compound integers are the powers of p.
Sketch of proof :
▷ we note $n = \overline{a_\ell\ a_{\ell-1}\ \ldots\ a_0}^p$ and we use Lucas's Theorem with specific k's to show that we must have $a_0 = a_1 = \ldots = a_{\ell-1} = 0$ and $a_\ell = 1$, which precisely means that $n = p^\ell$
▷ if $n = p^\ell$, then for each $1 \leqslant k \leqslant n-1$, there exists a non-zero digit b_i of k in base p and using once again Lucas's Theorem gives $\binom{p^\ell}{k} \equiv \binom{1}{0} \prod_{i=0}^{\ell-1} \binom{0}{b_i} \equiv 0 \mod p$ and show the equivalence. ∎

1. a) $\{p\}$-compoundness with p a prime

Claim :
The only $\{p\}$-compound integers are the powers of p.
Sketch of proof :
$\triangleright$ we note $n = \overline{a_\ell \ a_{\ell-1} \ \ldots \ a_0}^p$ and we use Lucas's Theorem with specific k's to show that we must have $a_0 = a_1 = \ldots = a_{\ell-1} = 0$ and $a_\ell = 1$, which precisely means that $n = p^\ell$
$\triangleright$ if $n = p^\ell$, then for each $1 \leqslant k \leqslant n-1$, there exists a non-zero digit b_i of k in base p and using once again Lucas's Theorem gives $\binom{p^\ell}{k} \equiv \binom{1}{0} \prod_{i=0}^{\ell-1} \binom{0}{b_i} \equiv 0 \mod p$ and show the equivalence. $\blacksquare$

1. b) 1-compoundness

Direct corollary :
an integer $n \geqslant 2$ is 1-compound if and only if $n = p^{\ell}$ for a certain prime number p and a certain $\ell \geqslant 1$.

2. a) Around S-compoundness for infinitely many $n \geqslant 2$: a)

S is a set of $\ell \geqslant 1$ prime numbers.

Proposition : There exist infinitely many S-compound integers $n \geqslant 2$.

Main idea : S-compoundness is preserved by inclusion.

Therefore to prove that there are infinitely many S-compound integers $n \geqslant 2$, it's sufficient to find $S' \subseteq S$ s.t. there are infinitely many S'-compound integers $n \geqslant 2$.

Since $\#S = \ell \geqslant 1$, there exists a prime number p in S, we choose $S' = \{p\}$, and by 1.a), each $n \in \{p^k \mid k \geqslant 1\}$ (an infinite set) is S'-compound. $\blacksquare$

2. a) Around S-compoundness for infinitely many $n \geqslant 2$: a)

S is a set of $\ell \geqslant 1$ prime numbers.

Proposition : There exist infinitely many S-compound integers $n \geqslant 2$.

Main idea : S-compoundness is preserved by inclusion.

Therefore to prove that there are infinitely many S-compound integers $n \geqslant 2$, it's sufficient to find $S' \subseteq S$ s.t. there are infinitely many S'-compound integers $n \geqslant 2$.

Since $\#S = \ell \geqslant 1$, there exists a prime number p in S, we choose $S' = \{p\}$, and by 1.a), each $n \in \{p^k \mid k \geqslant 1\}$ (an infinite set) is S'-compound. ■

2. a) Around S-compoundness for infinitely many $n \geqslant 2$: a)

S is a set of $\ell \geqslant 1$ prime numbers.

Proposition : There exist infinitely many S-compound integers $n \geqslant 2$.

Main idea : S-compoundness is preserved by inclusion.

Therefore to prove that there are infinitely many S-compound integers $n \geqslant 2$, it's sufficient to find $S' \subseteq S$ s.t. there are infinitely many S'-compound integers $n \geqslant 2$.

Since $\#S = \ell \geqslant 1$, there exists a prime number p in S, we choose $S' = \{p\}$, and by 1.a), each $n \in \{p^k \mid k \geqslant 1\}$ (an infinite set) is S'-compound. ■

2. a) Around S-compoundness for infinitely many $n \geqslant 2$: a)

S is a set of $\ell \geqslant 1$ prime numbers.

Proposition : There exist infinitely many S-compound integers $n \geqslant 2$.

Main idea : S-compoundness is preserved by inclusion.

Therefore to prove that there are infinitely many S-compound integers $n \geqslant 2$, it's sufficient to find $S' \subseteq S$ s.t. there are infinitely many S'-compound integers $n \geqslant 2$.

Since $\#S = \ell \geqslant 1$, there exists a prime number p in S, we choose $S' = \{p\}$, and by 1.a), each $n \in \{p^k \mid k \geqslant 1\}$ (an infinite set) is S'-compound. ■

2. b) Around S-compoundness for infinitely many $n \geqslant 2$

Claim :
There are infinitely many non S-compound integers $n \geqslant 2$.

Sketch of proof :
We set $A = \{n \geqslant 2 \mid \forall p \in S, p \nmid n\}$, and we show :
▷ A is an infinite set
▷ for each $n \in A$, n is not S-compound. ■

2. b) Around S-compoundness for infinitely many $n \geqslant 2$

Claim :
There are infinitely many non S-compound integers $n \geqslant 2$.

Sketch of proof :
We set $A = \{n \geqslant 2 \mid \forall p \in S, p \nmid n\}$, and we show :
▷ A is an infinite set
▷ for each $n \in A$, n is not S-compound. ∎

2. b) Around S-compoundness for infinitely many $n \geqslant 2$

Claim :
There are infinitely many non S-compound integers $n \geqslant 2$.

Sketch of proof :
We set $A = \{n \geqslant 2 \mid \forall p \in S, p \nmid n\}$, and we show :
▷ A is an infinite set
▷ for each $n \in A$, n is not S-compound. ■

3. a) Around 2-compoundness when $n = p^\alpha + 1$

Proposition : If $n = p^\alpha + 1$ with p a prime number and $\alpha \geqslant 1$, then n is 2-compound.

Sketch of proof : We actually show that n is $\{p, q\}$-compound where q is any prime divisor of n.

$\triangleright$ if $2 \leqslant k \leqslant n-2$, then $p \mid \binom{p^\alpha}{k-1}, \binom{p^\alpha}{k}$ by 1.a) so $p \mid \binom{p^\alpha}{k-1} + \binom{p^\alpha}{k} = \binom{p^\alpha+1}{k} = \binom{n}{k}$

$\triangleright$ if $k = 1$ or $k = n-1$, then $q \mid \binom{n}{k} = n$. $\blacksquare$

3. a) Around 2-compoundness when $n = p^\alpha + 1$

Proposition : If $n = p^\alpha + 1$ with p a prime number and $\alpha \geqslant 1$, then n is 2-compound.

Sketch of proof : We actually show that n is $\{p, q\}$-compound where q is any prime divisor of n.

▷ if $2 \leqslant k \leqslant n-2$, then $p \mid \binom{p^\alpha}{k-1}, \binom{p^\alpha}{k}$ by 1.a) so $p \mid \binom{p^\alpha}{k-1} + \binom{p^\alpha}{k} = \binom{p^\alpha+1}{k} = \binom{n}{k}$

▷ if $k = 1$ or $k = n-1$, then $q \mid \binom{n}{k} = n$. ■

3. a) Around 2-compoundness when $n = p^\alpha + 1$

Proposition : If $n = p^\alpha + 1$ with p a prime number and $\alpha \geqslant 1$, then n is 2-compound.

Sketch of proof : We actually show that n is $\{p, q\}$-compound where q is any prime divisor of n.

▷ if $2 \leqslant k \leqslant n-2$, then $p \mid \binom{p^\alpha}{k-1}, \binom{p^\alpha}{k}$ by 1.a) so $p \mid \binom{p^\alpha}{k-1} + \binom{p^\alpha}{k} = \binom{p^\alpha+1}{k} = \binom{n}{k}$

▷ if $k = 1$ or $k = n-1$, then $q \mid \binom{n}{k} = n$. ■

3. b) Around 2-compoundness when $n < p_s^{\alpha_s} + q(n)$

Here we have the prime factorisation $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ with $p_1^{\alpha_1} < \ldots < p_s^{\alpha_s}$.

We denote by $q(n)$ the largest prime less than n.

Proposition : If $n < q(n) + p_s^{\alpha_s}$, then n is 2-compound.

We did not send a proof for this proposition, but we have some ideas.

3. b) Around 2-compoundness when $n < p_s^{\alpha_s} + q(n)$

Here we have the prime factorisation $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ with $p_1^{\alpha_1} < \ldots < p_s^{\alpha_s}$.

We denote by $q(n)$ the largest prime less than n.
Proposition : If $n < q(n) + p_s^{\alpha_s}$, then n is 2-compound.

We did not send a proof for this proposition, but we have some ideas.

3. b) Around 2-compoundness when $n < p_s^{\alpha_s} + q(n)$

Here we have the prime factorisation $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ with $p_1^{\alpha_1} < \ldots < p_s^{\alpha_s}$.

We denote by $q(n)$ the largest prime less than n.
Proposition : If $n < q(n) + p_s^{\alpha_s}$, then n is 2-compound.

We did not send a proof for this proposition, but we have some ideas.

Thank for listening !

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 220 495 792 924 792 495 220 66 12 1
1 13 78 286 715 1287 1716 1716 1287 715 286 78 13 1
1 14 91 364 1001 2002 3003 3432 3003 2002 1001 364 91 14 1
1 15 105 455 1365 3003 5005 6435 6435 5005 3003 1365 455 105 15 1
1 16 120 560 1820 4368 8008 11440 12870 11440 8008 4368 1820 560 120 16 1
1 17 136 680 2380 6188 12376 19448 24310 24310 19448 12376 6188 2380 680 136 17 1
1 18 153 816 3060 8568 18564 31824 43758 48620 43758 31824 18564 8568 3060 816 153 18 1
1 19 171 969 3876 11628 27132 50388 75582 92378 92378 75582 50388 27132 11628 3876 969 171 19 1
1 20 190 1140 4845 15504 38760 77520 125970 167960 184756 167960 125970 77520 38760 15504 4845 1140 190 20 1
1 21 210 1330 5985 20349 54264 116280 203490 293930 352716 352716 293930 203490 116280 54264 20349 5985 1330 210 21 1
1 22 231 1540 7315 26334 74613 170544 319770 497420 646646 705432 646646 497420 319770 170544 74613 26334 7315 1540 231 22 1
1 23 253 1771 8855 33649 100947 245157 490314 817190 1144066 1352078 1352078 1144066 817190 490314 245157 100947 33649 8855 1771 253 23 1
1 24 276 2024 10626 42504 134596 346104 735471 1307504 1961256 2496144 2704156 2496144 1961256 1307504 735471 346104 134596 42504 10626 2024 276 24 1
1 25 300 2300 12650 53130 177100 480700 1081575 2042975 3268760 4457400 5200300 5200300 4457400 3268760 2042975 1081575 480700 177100 53130 12650 2300 300 25 1
1 26 325 2600 14950 65780 230230 657800 1562275 3124550 5311735 7726160 9657700 10400600 9657700 7726160 5311735 3124550 1562275 657800 230230 65780 14950 2600 325 26 1
1 27 351 2925 17550 80730 296010 888030 2220075 4686825 8436285 13037895 17383860 20058300 20058300 17383860 13037895 8436285 4686825 2220075 888030 296010 80730 17550 2925 351 27 1
1 28 378 3276 20475 98280 376740 1184040 3108105 6906900 13123110 21474180 30421755 37442160 40116600 37442160 30421755 21474180 13123110 6906900 3108105 1184040 376740 98280 20475 3276 378 28 1
1 29 406 3654 23751 118755 475020 1560780 4292145 10015005 20030010 34597290 51895935 67863915 77558760 77558760 67863915 51895935 34597290 20030010 10015005 4292145 1560780 475020 118755 23751 3654 406 29 1

Some ideas...

When $n < q(n) + p_s^{\alpha_s}$:

By symmetry, since $\binom{n}{k} = \binom{n}{n-k}$, it is sufficient to satisfy the divisibility condition for $k \leqslant n/2 \leqslant n-k$.

▷ if $q(n) > n-k$, then $q(n)$ is coprime to $k!$ and $(n-k)!$ and divides $n!$, so it divides $\frac{n!}{k!(n-k)!} = \binom{n}{k}$

▷ if $q(n) \leqslant n-k$, then $n - q(n) \geqslant k$ so $k < p_s^{\alpha_s}$ and so by Lucas's Theorem :

$$\binom{n}{k} \equiv \prod_{i=\alpha_s}^{\ell} \binom{a_i}{0} \prod_{i=0}^{\alpha_s - 1} \binom{0}{b_i} \equiv 0 \mod p_s$$

Thus n is $\{q(n), p_s\}$-compound so 2-compound. ∎

Some ideas...

When $n < q(n) + p_s^{\alpha_s}$:

By symmetry, since $\binom{n}{k} = \binom{n}{n-k}$, it is sufficient to satisfy the divisibility condition for $k \leqslant n/2 \leqslant n - k$.

$\triangleright$ if $q(n) > n - k$, then $q(n)$ is coprime to $k!$ and $(n-k)!$ and divides $n!$, so it divides $\frac{n!}{k!(n-k)!} = \binom{n}{k}$

$\triangleright$ if $q(n) \leqslant n - k$, then $n - q(n) \geqslant k$ so $k < p_s^{\alpha_s}$ and so by Lucas's Theorem :

$$\binom{n}{k} \equiv \prod_{i=\alpha_s}^{\ell} \binom{a_i}{0} \prod_{i=0}^{\alpha_s - 1} \binom{0}{b_i} \equiv 0 \mod p_s$$

Thus n is $\{q(n), p_s\}$-compound so 2-compound. ■

Some ideas...

When $n < q(n) + p_s^{\alpha_s}$:

By symmetry, since $\binom{n}{k} = \binom{n}{n-k}$, it is sufficient to satisfy the divisibility condition for $k \leqslant n/2 \leqslant n - k$.

▷ if $q(n) > n - k$, then $q(n)$ is coprime to $k!$ and $(n-k)!$ and divides $n!$, so it divides $\frac{n!}{k!(n-k)!} = \binom{n}{k}$

▷ if $q(n) \leqslant n - k$, then $n - q(n) \geqslant k$ so $k < p_s^{\alpha_s}$ and so by Lucas's Theorem :

$$\binom{n}{k} \equiv \prod_{i=\alpha_s}^{\ell} \binom{a_i}{0} \prod_{i=0}^{\alpha_s - 1} \binom{0}{b_i} \equiv 0 \mod p_s$$

Thus n is $\{q(n), p_s\}$-compound so 2-compound. ■

Some ideas...

When $n < q(n) + p_s^{\alpha_s}$:

By symmetry, since $\binom{n}{k} = \binom{n}{n-k}$, it is sufficient to satisfy the divisibility condition for $k \leqslant n/2 \leqslant n-k$.

▷ if $q(n) > n-k$, then $q(n)$ is coprime to $k!$ and $(n-k)!$ and divides $n!$, so it divides $\frac{n!}{k!(n-k)!} = \binom{n}{k}$

▷ if $q(n) \leqslant n-k$, then $n - q(n) \geqslant k$ so $k < p_s^{\alpha_s}$ and so by Lucas's Theorem :

$$\binom{n}{k} \equiv \prod_{i=\alpha_s}^{\ell} \binom{a_i}{0} \prod_{i=0}^{\alpha_s - 1} \binom{0}{b_i} \equiv 0 \mod p_s$$

Thus n is $\{q(n), p_s\}$-compound so 2-compound. ■

Some ideas...

Another useful tool :
Kummer's Theorem

Let p a prime and non-negative integers $n \geqslant k$. Then $\nu_p\left(\binom{n}{k}\right)$ is the number of carries when adding k and $n-k$ is base p.

Some ideas...

Another useful tool :
Kummer's Theorem

Let p a prime and non-negative integers $n \geqslant k$. Then $\nu_p\left(\binom{n}{k}\right)$ is the number of carries when adding k and $n-k$ is base p.